The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2001–2002

The Privacy Commissioner of Canada

Commissaire à la protection de la vie privée du Canada

Annual Report to Parliament 2001-2002

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-8210, 1-800-282-1376
Fax (613) 947-6850
TDD (613) 992-9190

Cat. No. IP30-1/2002
ISBN 0-662-66668-2

This publication is also available on our Web site at **www.privcom.gc.ca**

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

January 2003

The Honourable Daniel Hays
The Speaker
The Senate of Canada

Dear Mr. Hays:

I have the honour to submit to Parliament my Annual Report which covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act* and from December 1 to 31, 2001 for the *Personal Information Protection and Electronic Documents Act*.

I had originally intended this report to be released last spring. The year 2002 was a tumultuous one for privacy, however, and I was reluctant to report to Parliament while major issues, particularly issues involving the crucial balance between privacy and security in the aftermath of September 11, remained unresolved. In keeping with my mandate as an ombudsman for the privacy rights of Canadians, I continued to seek resolutions of these issues with ministers and senior public servants. To date, despite repeatedly extending my deadlines, I have not been successful. Obviously, I cannot ask Parliament to wait indefinitely, and must submit my report despite this inconclusive and unsatisfactory state of affairs.

I will report on the experience with the second year of the *Personal Information Protection and Electronic Documents Act* in my next annual report.

Yours sincerely,

George Radwanski
Privacy Commissioner of Canada

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Télec.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

103-03208/

January 2003

The Honourable Peter Milliken
The Speaker
The House of Commons

Dear Mr. Milliken:

I have the honour to submit to Parliament my Annual Report which covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act* and from December 1 to 31, 2001 for the *Personal Information Protection and Electronic Documents Act*.

I had originally intended this report to be released last spring. The year 2002 was a tumultuous one for privacy, however, and I was reluctant to report to Parliament while major issues, particularly issues involving the crucial balance between privacy and security in the aftermath of September 11, remained unresolved. In keeping with my mandate as an ombudsman for the privacy rights of Canadians, I continued to seek resolutions of these issues with ministers and senior public servants. To date, despite repeatedly extending my deadlines, I have not been successful. Obviously, I cannot ask Parliament to wait indefinitely, and must submit my report despite this inconclusive and unsatisfactory state of affairs.

I will report on the experience with the second year of the *Personal Information Protection and Electronic Documents Act* in my next annual report.

Yours sincerely,

George Radwanski
Privacy Commissioner of Canada

Table of Contents

Commissioner's Overview 1

Part One – Report on the *Privacy Act* 19

Introduction 19

Investigations 20

Complaints under the *Privacy Act* 20

Definitions of Findings under the *Privacy Act* 21

Summary of Select Cases under the *Privacy Act* 22

Departments accountable for information collected under contract 22

RCMP charges fee for traffic analysis report 24

DND improperly retains, uses information about pardoned convictions 25

CMHC's demand for tax information inappropriate 26

Inappropriate monitoring of employees' e-mail accounts 27

Man denied access to his information following war crimes investigation 29

Disclosure of information during appeal should be limited 30

Canada Post changes stance on using negative consent to sell addresses to mass mailers 32

Incidents under the *Privacy Act* 33

Improper disclosure of SIN on Canada Child Tax Benefit forms 34

Gun registry documents found in dumpster 34

HRDC/CCRA to share data on eligibility for Guaranteed Income Supplement 35

Public Interest Disclosures 36

Privacy Practices and Reviews 44
Introduction 44
Update on Canadian Firearms Program 45
Update on HRDC Governance protocol for the Databank Review Committee 47
In the Courts 49
Introduction 49
Traveller Declaration Forms (Form E-311) 49
Information Commissioner of Canada v. Commissioner of the RCMP and Privacy Commissioner 50
Clayton Charles Ruby v. Solicitor General 51
Robert Lavigne v. Office of the Commissioner of Official Languages 52
Information Commissioner of Canada v. Minister of Citizenship and Immigration Canada and Philip W. Pirie 52
Mertie Anne Beatty et al. v. the Chief Statistician et al. 53
Part Two – Report on the *Personal Information Protection and Electronic Documents Act* 55
Introduction 55
The Definition of Personal Information: Broad but not Infinite 55
Systemic Problems 57
Privacy code only the beginning 57
Not designating a privacy officer 58
Not knowing how to handle access requests and complaints 58
Keeping information too long or not long enough 58
Not meeting the time limit 58
Not limiting collection to what is necessary 59
Not identifying purpose for which information collected 59
Not instituting proper safeguards 60
Not recognizing that employees have privacy rights too 60
Positive Responses to my Recommendations 61
Definitions of Findings under the *PIPED Act* 61

Privacy Practices and Reviews 62

In the Courts 62

Mathew Englander v. Telus Communications Inc. 63

Ronald G. Maheu v. IMS Health Canada and the Privacy Commissioner of Canada 63

Communications and Public Education 64

Speaking engagements 64

Media relations 65

Public education materials 65

Advertising 66

Public inquiries 66

Web site 66

Part Three – Corporate Services 71

Resources 72

Detailed Expenditures 73

Corporate Structure 74

Commissioner's Overview

It is my duty, in this Annual Report, to present a solemn and urgent warning to every Member of Parliament and Senator, and indeed to every Canadian:

The fundamental human right of privacy in Canada is under assault as never before. Unless the Government of Canada is quickly dissuaded from its present course by Parliamentary action and public insistence, we are on a path that may well lead to the permanent loss not only of privacy rights that we take for granted but also of important elements of freedom as we now know it.

We face this risk because of the implications, both individual and cumulative, of a series of initiatives that the Government has mounted or is actively moving toward. These initiatives are set against the backdrop of September 11, and anti-terrorism is their purported rationale. But the aspects that present the greatest threat to privacy either have nothing at all to do with anti-terrorism, or they present no credible promise of effectively enhancing security.

The Government is, quite simply, using September 11 as an excuse for new collections and uses of personal information about all of us Canadians that cannot be justified by the requirements of anti-terrorism and that, indeed, have no place in a free and democratic society.

As of the date this Report went to press, January 17, the Government has shown no willingness to modify these initiatives in response to privacy concerns. Whether the Government's awareness of the imminence of this Report will have brought about any change by the time the Report is tabled, I cannot foresee.

I wish to emphasize at the outset that I have never once raised privacy objections against a single actual anti-terrorist security measure. Indeed, I have stated repeatedly ever since September 11 that I would never seek as Privacy Commissioner to stand in the way

George Radwanski
Privacy Commissioner of Canada

of any measures that might be legitimately necessary to enhance security against terrorism, even if they involved some new intrusion or limitation on privacy.

I have objected only to the extension of purported anti-terrorism measures to additional purposes completely unrelated to anti-terrorism, or to intrusions on privacy whose relevance or necessity with regard to anti-terrorism has not been in any way demonstrated. And still the Government is turning a resolutely deaf ear.

Specifically, I am referring to: the Canada Customs and Revenue Agency's new "Big Brother" passenger database; the provisions of section 4.82 of Bill C-17; dramatically enhanced state powers to monitor our communications, as set out in the "Lawful Access" consultation paper; a national ID card with biometric identifiers, as advanced by Citizenship and Immigration Minister Denis Coderre; and the Government's support of precedent-setting video surveillance of public streets by the RCMP.

These initiatives are all cause for deep concern because of the intrusions on privacy that they directly entail. But they are even more disturbing because of the thresholds they cross and the doors they open. Each of these measures establishes a devastatingly dangerous new principle of acceptable privacy invasion.

The CCRA's database introduces the creation of personal information dossiers on all law-abiding citizens for a wide variety of investigative purposes. Section 4.82 of Bill C-17 requires, for the first time, de facto mandatory self-identification to the police for general law enforcement. The "Lawful Access" paper advocates the widespread monitoring of our communications activities and reading habits.

A national ID card would remove our right to anonymity in our day-to-day lives. The RCMP's video surveillance constitutes systematic observation of citizens by the police as we go about our law-abiding business on public streets.

These are not abstract or theoretical concerns. If these measures are allowed to go forward and the privacy-invasive principles they represent are accepted, there is a very real prospect that before long our lives here in Canada will look like this:

- All our travels outside Canada will be systematically recorded, tracked and analyzed for signs of anything that the Government might find suspicious or undesirable. "Big Brother" dossiers of personal information about every law-abiding Canadian – initially travel information, but eventually supplemented by who knows what else – will be kept by the federal Government and will be available to virtually every federal department and agency, just in case they are ever handy to use against us.

IF THE GOVERNMENT'S CURRENT INITIATIVES ARE ALLOWED TO GO FORWARD, THERE IS A VERY REAL RISK THAT PRIVACY AS WE KNOW IT WILL SOON BECOME A DISTANT, IRRETRIEVABLE MEMORY.

- Any time we travel within Canada, we will have to identify ourselves to police so that their computers can check whether we are wanted for anything or are otherwise of interest to the state.
- Police and security will be able to access records of every e-mail we send and every cellular phone call we make. Information on what we read on the Internet, every Web site and page we visit, will likewise be readily available to government authorities.
- We will all be fingerprinted or retina-scanned by the Government. This biometric information will be on compulsory national ID cards that will open the way to being stopped in the streets by police and required to identify ourselves on demand.
- Our movements through the public streets will be relentlessly observed through proliferating police video surveillance cameras. Eventually, these cameras will likely be linked to biometric face-recognition technologies that will match our on-screen images to file photos – from such sources as drivers' licences, passports or ID cards – and enable the police to identify us by name and address as we go about our law-abiding business in the streets.

I am well aware that these scenarios are likely to sound, to most people, like alarmist exaggeration. Certainly, the society I am describing bears no relation to the Canada we know. But anyone who is inclined to dismiss the risks out of hand should pause first to consider that the privacy-invasive measures already being implemented or developed right now would have been considered unthinkable in our country just a short year ago.

I am not predicting that all this will necessarily happen. But I am warning with all the intensity at my disposal that, in each instance, once the principle has been accepted and the precedent has been established, further intrusions on privacy are only a matter of degree. That makes them virtually inevitable.

The place to stop unjustified intrusions on a fundamental human right such as privacy is right at the outset, at the very first attempt to enter where the state has no business treading. Otherwise, the terrain will have been conceded, and the battle lost.

Consequently, if the Government's current initiatives are allowed to go forward, there is a very real risk that privacy as we know it will soon become a distant, irretrievable memory.

The situation is made all the more worrisome by the fact that the Government is doing all this in blatant, open and repeated disregard of the concerns that it is my duty to express as the Officer of Parliament mandated to oversee and defend the privacy rights of all Canadians.

This disregard threatens the privacy rights of Canadians not only directly through the intrusive measures in question, but also

indirectly by undermining the whole edifice of privacy protection that has been in place in this country for nearly two decades.

Regrettably, this Government has lost its moral compass with regard to the fundamental human right of privacy.

It appears to have become convinced that privacy must be sacrificed bit by bit, day by day, in pursuit of greater goods: reassuring a public frightened by the outrages of September 11; mollifying an insistent U.S. government; meeting the wishes of police, security forces and other Government institutions that have recognized the aftermath of September 11 as an opportunity to expand their powers.

As well, the Government has become inappropriately willing to brush aside all criticism of its assault on privacy rights, apparently regarding such criticism as simply a cost of doing business. This criticism has come not only from me in the exercise of my mandate from Parliament to oversee and defend the privacy rights of Canadians, but also from a great many others who have publicly endorsed my concerns. These include seven provincial and territorial Information and Privacy Commissioners from across Canada, the Canadian Civil Liberties Association, the B.C. Civil Liberties Association, the B.C. Freedom of Information and Privacy Association, the *Ligue des droits et libertés*, Electronic Frontier Canada, the Commonwealth Centre for e-Governance, the Public Interest Advocacy Centre, and the Manitoba Association of Rights and Liberties.

In the nearly 20-year history of privacy protection since the position of Privacy Commissioner was created under the *Privacy Act* in 1983, a convention has been established that when the Privacy Commissioner points out that a practice or an initiative is inconsistent with privacy rights, the Government pays heed.

That's the way the system is supposed to work. I am an ombudsman, mandated by Parliament, whose role with regard to the federal Government is normally carried out primarily through persuasion and co-operative discussion behind the scenes. Like my predecessors, that is the way I have sought to operate since my appointment. I have recommended to ministers and senior Government officials specific solutions to enable them to achieve their legitimate policy objectives in ways that are more respectful of privacy rights. This has produced many successful outcomes which, by the very nature of the process, do not come publicly to light.

But in its approach to the aftermath of September 11, the Government has increasingly been turning its back on the cooperative nature of the federal privacy protection system by flatly refusing to pay attention. In each of the instances where I have been obliged to publicly criticize the Government for failing to respect the privacy rights of Canadians,

GOVERNMENTAL DISREGARD FOR CRUCIALLY IMPORTANT PRIVACY RIGHTS IS MOVING BEYOND ISOLATED INSTANCES AND BECOMING SYSTEMATIC. THIS PUTS A FUNDAMENTAL RIGHT OF EVERY CANADIAN PROFOUNDLY AT RISK.

it was only after I had first made every effort to persuade the minister responsible with carefully reasoned arguments and had my expressions of concern ignored or brushed aside.

Now I am informing Parliament that there is every appearance that governmental disregard for crucially important privacy rights is moving beyond isolated instances and becoming systematic. This puts a fundamental right of every Canadian profoundly at risk. It is a trend that urgently needs to be reversed.

If the Government can, with impunity and without provoking the strongest response from Parliament, simply brush aside the Privacy Commissioner's warnings and do as it pleases, then privacy protection in this country will be progressively weakened, and worse and worse intrusions will be inevitable.

In the months immediately following September 11, I was in fact quite optimistic that, with regard to privacy, the Government was on the whole being balanced and thoughtful in its response. But now the floodgates appear to have burst.

Now "September 11" is invoked as a kind of magic incantation to stifle debate, disparage critical analysis and persuade us that we live in a suddenly new world where the old rules cannot apply.

If Parliament and the public at large have been slow to react, it is probably because for most people, most of the time, privacy is a pretty abstract concept. Like our health, it's something we tend not to think about until we lose it – and then discover that our lives have been very unpleasantly, and perhaps irretrievably, altered.

But though we tend to take it for granted, privacy – the right to control access to ourselves and to personal information about us – is at the very core of our lives. It is a fundamental human right precisely because it is an innate human need, an essential condition of our freedom, our dignity and our sense of well-being.

If someone intrudes on our privacy – by peering into our home, going through the personal things in our office desk, reading over our shoulder on a bus or airplane, or eavesdropping on our conversation – we feel uncomfortable, even violated.

Imagine, then, how we will feel if it becomes routine for bureaucrats, police officers and other agents of the state to paw through all the details of our lives: where and when we travel, and with whom; who are the friends and acquaintances with whom we have telephone conversations or e-mail correspondence; what we are interested in reading or researching; where we like to go and what we like to do.

THE RIGHT NOT TO BE KNOWN AGAINST OUR WILL – INDEED, THE RIGHT TO BE ANONYMOUS EXCEPT WHEN WE CHOOSE TO IDENTIFY OURSELVES – IS AT THE VERY CORE OF HUMAN DIGNITY, AUTONOMY AND FREEDOM.

A popular response is: "If you have nothing to hide, you have nothing to fear."

By that reasoning, of course, we shouldn't mind if the police were free to come into our homes at any time just to look around, if all our telephone conversations were monitored, if all our mail were read, if all the protections developed over centuries were swept away. It's only a difference of degree from the intrusions already being implemented or considered.

The truth is that we *all* do have something to hide, not because it's criminal or even shameful, but simply because it's private. We carefully calibrate what we reveal about ourselves to others. Most of us are only willing to have a few things known about us by a stranger, more by an acquaintance, and the most by a very close friend or a romantic partner. The right not to be known against our will – indeed, the right to be anonymous except when we choose to identify ourselves – is at the very core of human dignity, autonomy and freedom.

If we allow the state to sweep away the normal walls of privacy that protect the details of our lives, we will consign ourselves psychologically to living in a fishbowl. Even if we suffered no other specific harm as a result, that alone would profoundly change how we feel. Anyone who has lived in a totalitarian society can attest that what often felt most oppressive was precisely the lack of privacy.

But there also will be tangible, specific harm.

The more information government compiles about us, the more of it will be wrong. That's simply a fact of life.

Several years ago, after the existence of Human Resources Development Canada's "Longitudinal Labour Force File" was brought to light by my predecessor, many people demanded to see the information that had been held about them. They were astonished by the number of factual errors. That was only a research database, so its inaccuracies probably would have remained relatively benign even if it had not been dismantled.

But if our privacy becomes ever more systematically invaded by the state for purposes of assessing our behavior and making judgments about us, wrong information and misinterpretations will have potential consequences.

If information that is actually about someone else is wrongly applied to us, if wrong facts make it appear that we've done things we haven't, if perfectly innocent behavior is misinterpreted as suspicious because authorities don't know our reasons or our circumstances, we will be at risk of finding ourselves in trouble in a society where everyone is regarded as a suspect. By the time we clear our names and establish our innocence, we may have suffered irreparable financial or social harm.

IF WE HAVE TO LIVE OUR LIVES WEIGHING EVERY ACTION, EVERY COMMUNICATION, EVERY HUMAN CONTACT, WONDERING WHAT AGENTS OF THE STATE MIGHT FIND OUT ABOUT IT, ANALYZE IT, JUDGE IT, POSSIBLY MISCONSTRUE IT, AND SOMEHOW USE IT TO OUR DETRIMENT, WE ARE NOT TRULY FREE.

Worse yet, we may never know what negative assumptions or judgments have been made about us in state files. Under exemptions to the general right of access under the *Privacy Act*, Canadians do not have the right to see the personal information that the Government holds about them if it pertains to national security or an ongoing investigation.

Decisions detrimental to us may be made on the basis of wrong facts, incomplete or out-of-context information or incorrect assumptions, without our ever having the chance to find out about it, let alone to set the record straight.

That possibility alone will, over time, make us increasingly think twice about what we do, where we go, with whom we associate, because we will learn to be concerned about how it might look to the ubiquitous watchers of the state.

- You stopped briefly in Thailand during a business trip, and liked it so much that you're thinking of going back on a vacation. But might repeat travel to Thailand get you flagged by the Government's analysts as a possible pedophile going there for the child sex trade? Could you find yourself detained for questioning every time you travel? Might you be denied security clearances, or refused entry into the United States?
- You're passing time browsing on the Internet and you're idly curious about what kind of propaganda in favour of al-Qaeda various extremists might be putting out. But could visiting such Web sites get you identified as a potential terrorist yourself and bring CSIS or RCMP officers knocking on your door?
- You're stopped on the street by a stranger asking for directions. But if by then proliferating street video surveillance cameras are linked to biometric face-recognition technology, what if the system immediately identifies the stranger as a known or suspected terrorist? If the police officer then calls up your name and address by matching your onscreen image to your driver's license or passport photo, will you go into security files yourself as a suspicious individual who had a street meeting with a terrorism suspect? Would you do better to keep walking whenever any stranger tries to talk to you?

The bottom line is this: If we have to live our lives weighing every action, every communication, every human contact, wondering what agents of the state might find out about it, analyze it, judge it, possibly misconstrue it, and somehow use it to our detriment, we are not truly free.

That sort of life is characteristic of totalitarian countries, not a free and open society like Canada. But that is where we are inexorably headed, if the Government's current initiatives are allowed to proceed.

Let me very briefly address the specifics of these objectionable initiatives, before suggesting some broader considerations that I believe should guide us in the post-September 11 environment.

The CCRA "Big Brother" database

In late 2001, under amendments to the *Customs Act*, Customs officers of the CCRA were given access to Advance Passenger Information (API) and the far more detailed Passenger Name Record (PNR) about every passenger flying into Canada from a foreign destination. The stated purpose of this was to facilitate identifying individuals who merit more careful questioning or examination on arrival.

When this legislation was before Parliament, I sought and received a formal written undertaking from the CCRA that, except in those relatively few instances where this API/PNR information did in fact cause an individual to be identified for secondary screening, it would all be destroyed within 24 hours. On the basis of this unequivocal undertaking that there would be no widespread retention, I did not express any privacy objection to providing Customs with this passenger information and did not find it necessary to appear before the House and Senate committees that studied the proposed amendments.

Last summer, the CCRA informed me that, contrary to its past undertaking, it has decided to keep all API/PNR information about Canadian travellers for six years in a massive new database.

All this personal information – more than 30 data elements including every destination to which we travel, who we travel with, how we pay for the tickets (sometimes including credit card numbers), what contact numbers we provide, even any dietary preferences or health-related requirements we communicate to the airline – will be available for an almost limitless range of governmental purposes under the broad information-sharing provisions of the *Customs Act*.

Those purposes, by the Government's own account, include everything from routine income tax investigations to trying to flag Canadians as potential pedophiles or money launderers solely on the basis of their travel patterns.

This is unprecedented. The Government of Canada has absolutely no business creating a massive database of personal information about all law-abiding Canadians that is collected without our consent from third parties, not to provide us with any service but simply to have it available to use against us if it ever becomes expedient to do so. Compiling

It is difficult to imagine a more flagrant disregard for the rights of Canadians. This database is legally wrong and morally wrong.

dossiers on the private activities of all law-abiding citizens is the sort of thing the Stasi secret police used to do in the former East Germany. It has no place in a free and democratic society.

The CCRA's purported reason for creating this database is "forensic": In the event that there is a terrorist attack and some of the perpetrators are known, it wants to be able to use this database in search of any accomplices or associates. The CCRA has absolutely no mandate under the *Customs Act* to gather information for this sort of after-the-fact anti-terrorist forensic investigation.

But I have repeatedly asked Revenue Minister Elinor Caplan at least to limit the uses of this database to this exceptional anti-terrorist purpose, by strictly exempting it from the normal information-sharing provisions of the *Customs Act*. She flatly refuses.

The creation of this CCRA database lacks Parliamentary authority. It contravenes the *Privacy Act*. And there is overwhelming reason to believe that it is contrary to the *Canadian Charter of Rights and Freedoms*.

I have provided to Minister Caplan and to the Government, and made public, three separate independent legal opinions from the most eminent of authorities: retired Supreme Court Justice Gérard V. La Forest, who wrote many of the Court's most important decisions on privacy rights; former federal Deputy Minister of Justice Roger Tassé, who played a key role in drafting the *Canadian Charter of Rights and Freedoms*; and Hon. Marc Lalonde, who was a highly respected Minister of Justice in the Trudeau cabinet. All three state that this database clearly appears to be in violation of the *Charter*. This unprecedented trilogy of opinions has met with apparent indifference.

It is difficult to imagine a more flagrant disregard for the rights of Canadians. This database is legally wrong and morally wrong. If the Government can get away with systematically logging and analyzing all the foreign travel activities of every law-abiding citizen, then no other private activity will long be safe from being included in the same personal dossiers – our shopping, our banking, our communications, our movements within the country. The "Big Brother" society will be irrevocably upon us.

Bill C-17, the *Public Safety Act, 2002*

In the *Public Safety Act, 2002*, Bill C-17, the Government has reintroduced, with only minimal changes, a provision from the previous Bill C-55 that would give the RCMP and CSIS unrestricted access to the personal information held by airlines about all Canadian air travellers on domestic as well as international flights.

I have raised no objection to the primary purpose of this provision, section 4.82, which is to enable the RCMP and CSIS to use this passenger information for anti-terrorist

IF THE POLICE WERE ABLE TO CARRY OUT THEIR REGULAR *CRIMINAL CODE* LAW ENFORCEMENT DUTIES WITHOUT THIS NEW POWER BEFORE SEPTEMBER 11, THEY SHOULD LIKEWISE BE ABLE TO DO SO NOW.

"transportation security" and "national security" screening. But my concern is that the RCMP would also be expressly empowered to use this information to seek out persons wanted on warrants for *Criminal Code* offences that have nothing to do with terrorism, transportation security or national security.

The implications of this are extraordinarily far-reaching. In Canada, it is well established that we are not required to identify ourselves to police unless we are being arrested or we are carrying out a licensed activity such as driving. This right to anonymity with regard to the state is a crucial privacy right. But since we are required to identify ourselves to airlines as a condition of air travel and since section 4.82 would give the RCMP unrestricted access to the passenger information obtained by airlines, this would set the extraordinarily privacy-invasive precedent of effectively requiring compulsory self-identification to the police.

I am prepared, though I seriously doubt its effectiveness, to accept this as an exceptional measure that can be justified in the wake of September 11 for the limited and specific purposes of aviation security and national security against terrorism. But I can find no reason why the use of this de facto self-identification to the police should be extended to searching for individuals who are of interest to the state because they are the subject of warrants for *Criminal Code* offences unrelated to terrorism. That has the same effect as requiring us to notify the police every time we travel, so that they can check whether we are wanted for something.

If the police were able to carry out their regular *Criminal Code* law enforcement duties without this new power before September 11, they should likewise be able to do so now.

If we accept, instead, the principle that air travellers within Canada can now in effect be forced by law to identify themselves to police for scrutiny against lists of wanted suspects, then there is nothing to prevent the same logic from being applied in future to other modes of transportation. Particularly since this provision might well discourage wanted individuals from travelling by air, why not extend the same scrutiny to train travellers, bus passengers or anyone renting a car?

Indeed, the precedent set by this provision could ultimately open the door to practices similar to those that exist in societies where police routinely board trains, establish roadblocks or stop people on the street to check identification papers in search of anyone of interest to the state.

This is why I have recommended amending the bill to remove all reference to warrants and thus limit the police to using this passenger information only to watch for individuals who are of concern specifically on grounds of anti-terrorism and national security.

When the Government reintroduced this legislation as Bill C-17, it made a number of changes. But my recommendations regarding section 4.82 were ignored. Instead, the Government made two changes that are at best cosmetic, and that appear aimed more at misleading Canadians than at addressing the real issues that are at stake.

The Government now proposes to have regulations limiting slightly the *Criminal Code* offence warrants for which the RCMP will be searching. But this does nothing to address the fundamental point of principle that the police have no business using this extraordinary access to personal information to search for people wanted on warrants for any offences unrelated to terrorism.

As well, in the new bill the Government has removed the "identification of persons for whom a warrant has been issued" as a "purpose" for accessing passenger information under the legislation. But this is meaningless, since the RCMP would remain empowered to match this information against a database of persons wanted on warrants and to use such matches to bring about arrests.

Senior Government officials have repeatedly told me that the reference to warrants is necessary, because otherwise the RCMP would be powerless to act if they "incidentally" came upon the name of a dangerous wanted criminal while scanning a passenger list for possible terrorists. This argument is totally unpersuasive for two reasons.

First, if RCMP officers are to examine passenger information for the sole stated purpose of looking for terrorists and security risks, they shouldn't be checking passenger names against the huge general CPIC database, which contains a very wide variety of information including the names of people wanted on all sorts of warrants completely unrelated to terrorism. They should be looking for matches against the much more specific database that is limited to information only on known or suspected terrorists and other individuals identified as security risks.

To say that trolling in CPIC might cause the RCMP to "incidentally" find individuals wanted on warrants for *Criminal Code* offences, is like saying that there is something "incidental" about tossing a fishing line into a pond stocked with trout and pulling out a trout.

Second, my legal advisors have confirmed that peace officers including the RCMP have a well-established Common Law power – indeed a duty – to take appropriate action to apprehend any potentially dangerous individual they discover to be wanted on a warrant. The reference to warrants in section 4.82 of Bill C-17 is therefore quite redundant and unnecessary – unless, of course, the RCMP are to make a systematic practice of searching passenger information for individuals wanted on outstanding warrants, contrary to the stated purpose of giving them access to this information.

THE INTERCEPTION AND MONITORING OF PRIVATE COMMUNICATIONS IS A HIGHLY INTRUSIVE ACTIVITY THAT STRIKES AT THE HEART OF THE RIGHT TO PRIVACY.

The "Lawful Access" Initiative

Under the "Lawful Access" proposals that have been put forward jointly by the Minister of Justice, the Solicitor General and the Minister of Industry, the Internet activities and cellular phone communications of all law-abiding Canadians would be subject to unprecedented scrutiny by the state.

I have responded formally, publicly and in detail to these proposals, and will not do so again here. But I have received absolutely no indication that the grave privacy concerns I have expressed will be heeded, and I have considerable reason to fear that the Government intends to simply press ahead.

The interception and monitoring of private communications is a highly intrusive activity that strikes at the heart of the right to privacy. If Canadians can no longer feel secure that their Web surfing and their electronic communications are indeed private, this will mark a grave, needless and unjustifiable deterioration of privacy rights in our country.

The Government has presented no evidence to demonstrate why the massive new intrusions it proposes are necessary.

I recognize that new information technologies may pose a challenge to conventional interception and surveillance techniques used by police forces and national security agencies. It appears reasonable that law enforcement and national security agencies should have the same ability to intercept and monitor e-mail and cellular telephone communications, with the same kind of judicial authorization based on the same criteria, as is now the case with regard to letter mail and conventional telephone communications.

But agents of the state in Canada cannot order Canada Post to photocopy the address on every envelope we send, nor can they order bookstores to keep a record of every book we buy, let alone of every page of every magazine we leaf through. There is no reason why they should be able to exercise such powers with regard to every e-mail someone sends or every Web site he or she visits.

I do not see any reason why e-mails should be subject to a lower standard of privacy protection than letters or telephone calls. And I do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a reference library. Canadians should not be subject to greater state monitoring or scrutiny just because they choose to use new communication technologies.

In a free and democratic society like Canada, the interception and monitoring of private communications carries extraordinarily strong symbolic and psychological implications, in addition to the obvious practical ones. Dramatically increasing that interception and monitoring, without any clearly demonstrated need or justification, is unacceptable.

I CAN FIND NO JUSTIFICATION FOR A NATIONAL IDENTITY CARD, ESPECIALLY SINCE IT IS ABSOLUTELY USELESS AS AN ANTI-TERRORIST MEASURE.

Identity Cards

It is a matter of very considerable dismay that Citizenship and Immigration Minister Denis Coderre, presumably on behalf of the Government, is pressing for a "debate" on establishing a mandatory national identity card, complete with biometric identifiers, for all Canadians.

Given the Government's current behavior on other privacy matters, it is difficult to avoid fearing that this means that it wishes to introduce such a card.

That would be another huge blow to privacy rights. In Canada, we are not required to carry *any* identification – let alone to identify ourselves on demand – unless we are carrying out a licensed activity such as driving. Introducing a national identity card, even if it were "voluntary" at first, would push us toward becoming the kind of society where the police can stop anyone on the street and demand, "Your papers, please."

The notion of the Government of Canada fingerprinting or eyeball-scanning every citizen for such a card is, of course, all the more abhorrent.

I can find no justification for a national identity card, especially since it is absolutely useless as an anti-terrorist measure. As the perpetrators of the September 11 attacks demonstrated, terrorists are not necessarily previously identifiable as such. Every citizen would be able to obtain and display an identity card, regardless of his or her possible terrorist proclivities, but of course it wouldn't list occupation as "terrorist." And short-term visitors to Canada wouldn't have such a card at all.

Rather than a "debate" about a grave and needless intrusion, Canada needs clear acknowledgement by the Government that the fundamental privacy right of anonymity as we go about our day-to-day lives is too important to abrogate for no apparent reason.

Video Surveillance

I have been trying for more than a year to persuade the Government to direct the RCMP to stop its continuous video surveillance of law-abiding citizens on a public street in Kelowna, British Columbia.

I believe that general video surveillance of our public streets and public gathering places by the police or other public authorities is an enormous threat to the fundamental human right of privacy in our society.

We have the right as Canadians to walk along our public streets without being systematically observed by police. If we lose that, we lose a crucial part of our privacy and our freedom.

Last March, I sought the advice of retired Supreme Court Justice Gérard La Forest, who wrote many of the Supreme Court's most important decisions on privacy rights. Mr. La Forest advised me that, in his learned opinion, what the RCMP is doing in Kelowna

is not only a serious violation of privacy rights, but is also a clear contravention of the *Canadian Charter of Rights and Freedoms*.

I made that legal opinion public last April, and it too was ignored by the RCMP and the Government. Since as Privacy Commissioner I am mandated by Parliament to oversee and defend the privacy rights of Canadians, and since I have the strongest possible reason to believe that what the RCMP is doing in Kelowna not only violates privacy rights in general but is unconstitutional, my only remaining recourse is to ask the courts to put a stop to it.

Accordingly, in July I initiated in the Supreme Court of British Columbia in Kelowna, an action to declare the RCMP's video surveillance activities in Kelowna unconstitutional as a violation of the *Canadian Charter of Rights and Freedoms* and international covenants.

Remarkably, the Government has taken the position that it challenges my right to take this action. It takes the position that as Privacy Commissioner I am a "statutory body" limited to doing only what is expressly spelled out in the *Privacy Act*.

My legal advisors inform me that they are confident that this position is not correct in law. But I have strong reason to believe that if my right to initiate this *Charter* challenge is upheld by the court, the Government intends to file a series of appeals with a view to preventing this important case from being heard on its merits for years to come.

That would be reprehensible. At a time when video surveillance of public streets is becoming a fad that appeals to many municipalities across Canada, Canadians are entitled to have this important question about their privacy rights under the *Charter* adjudicated without delay. As well, police forces and municipalities across the country should themselves not be subjected to prolonged and needless uncertainty about the constitutional legality of what they are contemplating. They want and need a court decision.

I have therefore repeatedly asked the Minister of Justice and Attorney General, Mr. Cauchon, to withdraw this procedural objection and allow the case to be promptly determined on its merits. I have recently been informed that he refuses to do this.

Instead the Government, through the Minister of Justice, is taking the extraordinary position that the Privacy Commissioner of Canada should not have the right to ask the courts to determine whether a grave intrusion on privacy violates the privacy protections in the *Canadian Charter of Rights and Freedoms*.

I urge the Government to reconsider.

'The United States made us do it' cannot be a sufficient or acceptable justification for the Government to intrude on a fundamental right of Canadians.

With regard to all these initiatives except street video surveillance, Government officials have repeatedly told me privately that pressure from the United States government is a strong motivating factor.

Let me be blunt: "The United States made us do it" cannot be a sufficient or acceptable justification for the Government to intrude on a fundamental right of Canadians.

Canada is a sovereign country.

Throughout our history, there have been important instances where Canada has found it necessary to take a position different from that of the United States on matters involving rights or values. It is surely no exaggeration to say that if our leaders had instead consistently succumbed to U.S. pressures to adopt that country's approaches as our own, there would today be no distinct Canada as we know it.

The same is true with regard to appropriate respect for fundamental rights in the wake of September 11. If the U.S. government is indeed exerting pressure on Canada to take steps that cannot be justified on their merits in accordance with our Canadian values and rights, then Canadians are entitled to expect that the Government will remain steadfast in meeting its responsibilities rather than trample on their rights out of fear of U.S. retaliation.

Canadians are entitled, as well, to expect that the Government will think very carefully and critically before accepting the U.S. premise that we are all "at war" against terrorism and that it is therefore reasonable to impose wartime restrictions on privacy and other rights.

The difficulty is that terrorism is not an enemy, but a phenomenon. Wars that are fought between nation-states, or even civil wars that are fought within a country, are finite. They may drag on for a long time, but eventually someone wins and someone loses or a stalemate is identified, and the terms of peace are established.

But if we apply the premises of war to the challenges of dealing with terrorism, we will by definition be committing ourselves to a "war" with no possible end – because there is no single, definable enemy. Any group of individuals, or even any single individual, that is willing to commit public mayhem in support of any particular cause is thereby a terrorist. And so for every particular group or faction of terrorists that is neutralized, another one may readily spring up.

This means that there can never be a moment when it will be possible to declare a definitive victory in a "war" against terrorism. In fact, such a "war" will be eerily reminiscent of Orwell's *1984*, which takes place against the background of a mysterious chronic war in which it is never clear just who the enemy is or who is winning or losing.

We need to recognize, therefore, that any intrusions or limitations on the fundamental human right of privacy that are imposed as a purported wartime measure against terrorism will likely never be rescinded. What we are confronting is the prospect of a permanent redefinition of Canadian society.

And what will this redefinition achieve in terms of protecting us?

The reality is that there are no security measures that can provide complete protection against murderous individuals or groups who are willing to lose their own lives to make their point. Even the most repressive, authoritarian regimes have not been able to immunize themselves fully against terrorism. At the same time, we also need to keep the risks in perspective: In any scenario, the average Canadian is far more likely to come to harm in a traffic accident than at the hands of terrorists.

This is not to suggest that we should take a cavalier approach to terrorism, but rather that we must take a balanced one.

When people are worried about their safety, when we have seen the horrors of which today's breed of terrorists are capable – and there may be more – it's easy to lose perspective. It's easy to fall into the trap of thinking that security is all that matters and that human rights such as privacy are a luxury.

But such extremes can only reward and encourage terrorism, not diminish it. They can only devastate our lives, without commensurately safeguarding them.

Of course we all want to be safe. But we could be safer from terrorism – perhaps – if we permanently evacuated all the high-rise office towers, if we closed down the subways, if we forever grounded all airplanes.

Yet no reasonable person would be likely to argue for adopting such measures. We'd say, "We want to be safe, yes – but not at the price of sacrificing our whole way of life."

The same reasoning should apply, in my view, to arguments that privacy should indiscriminately be sacrificed on the altar of enhanced security.

The essence of terrorism is the impact it is intended to have on those who witness it – the capacity to frighten, to demoralize, to sap the will of a society to resist whatever it is that the terrorists want.

In the case of the September 11 breed of terrorists, by all accounts it is the whole nature of American society, and by extension of all our Western societies, that they seek to attack and undermine. Our freedoms and values, very much including privacy, are precisely the target.

To keep that from becoming a reality for Canada, we must guard against falling prey to the illusion that wholesale erosion of privacy is a reasonable, necessary or effective way to enhance security.

WE MUST GUARD AGAINST THE EAGERNESS OF LAW ENFORCEMENT BODIES AND OTHER AGENCIES OF THE STATE TO USE THE RESPONSE TO SEPTEMBER 11 AS A TROJAN HORSE FOR ACQUIRING NEW INVASIVE POWERS.

We must guard against the demonstrated tendency of the Government to create new databases of privacy-invasive information on justified, exceptional grounds of enhancing security, and then seek to use that information for a whole range of other law enforcement or governmental purposes that have nothing to do with anti-terrorism – simply because it's there.

And we must guard against the eagerness of law enforcement bodies and other agencies of the state to use the response to September 11 as a Trojan horse for acquiring new invasive powers or abolishing established safeguards simply because it suits them to do so.

Perhaps it will be necessary to accept some new intrusive measures to enhance security. But these choices must be made calmly, carefully and case by case. The burden of proof must always be on those who suggest that some new intrusion or limitation on privacy is needed in the name of security.

I have suggested that any such proposed measure must meet a four-part test:

It must be demonstrably necessary in order to meet some specific need.

It must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer.

The intrusion on privacy must be proportional to the security benefit to be derived.

And it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

Necessity, effectiveness, proportionality, and lack of a less privacy-invasive alternative – this is the four-part test that I believe can allow us to take all appropriate measures to enhance security, without unduly sacrificing privacy. It is a test on which I believe all of us – every Canadian, and particularly every Member of Parliament and Senator, of every party and every political philosophy – must resolutely insist.

One of the clearest lessons of history is that the greatest threats to liberty come not when times are tranquil and all is well, but in times of turmoil, when fidelity to values and principle seems an extravagance we can ill afford. History also teaches us that whenever we have given in to that kind of thinking, we have lived to regret it.

At the time, the loss of freedom might seem small, trivial even, when placed in the balance of the security we seek. And yet these incremental threats are the ones we must be most vigilant in resisting. The 18th Century political philosopher Edmund Burke understood this danger when he wrote, "The true danger is when liberty is nibbled away, for expedience, and by parts."

U.S. Supreme Court Justice Thurgood Marshall eloquently made the same point much more recently when he said: "History teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure."

We are now living in such a time. Canada has, over the course of its history, developed a very healthy balance between the powers of the state and the rights of the individual. Our crime rates have been comparatively low and our social order has been strong, while individual freedom and diversity have flourished to a degree that is the envy of much of the world. That is why immigrants from so many other societies have chosen to make Canada their home.

But now we face having that successful balance changed, by having Canada transformed into a society where the state is much more intrusive and where individual rights and freedoms are correspondingly reduced. And we face having this transformation occur without the analysis, debate or even understanding that it deserves.

Sadly, most of the ministers who are making these decisions are not thinking sufficiently about the deeper implications of what they are doing. While I am continuing to maintain dialogue with the relevant officials in pursuit of appropriate changes, at the time this Report goes to press no discernible progress has been made.

Even with the help and support of my provincial and territorial colleagues, other privacy advocates and many thoughtful members of the news media – to all of whom I am profoundly grateful – as an ombudsman I do not have the power to stop what the Government is doing in its unprecedented assault on privacy.

That power lies in Parliamentary insistence and public outcry. It is my hope that these will be exercised with the greatest urgency. It is also my hope that, even at this late moment, the Government will have the courage and the good sense to recognize that there is no shame in rethinking and revising insufficiently-considered policies. There can be shame only in insisting, instead, on treading needlessly on a fundamental right of Canadians.

For my part, my role and my duty are to bear true witness to what is taking place, and to fight against it with every appropriate means available to me. This I will continue to do ceaselessly, and with all the vigour at my disposal.

Part One
Report on the *Privacy Act*

Introduction

The *Privacy Act* protects individuals' privacy with respect to personal information held by federal Government institutions.

The *Act*, which has been in force since 1983, governs how federal institutions collect, use, disclose and dispose of personal information, and gives people the right to access and request corrections to their personal information.

As Privacy Commissioner, I receive and investigate complaints from individuals who believe their rights under the *Act* have been violated. I can also initiate a complaint and an investigation myself, in any situation where there are reasonable grounds to believe the *Act* has been violated.

First and foremost, I am an ombudsman, and whenever possible, complaints are resolved through mediation and negotiation. But I also have broad powers of investigation under the *Act*. As Privacy Commissioner I can subpoena witnesses, compel testimony and enter premises to obtain documents and conduct interviews. Obstructing one of my investigations is an offence under the *Act*. Although the *Act* does not include the power to order compliance, I can recommend changes to the way Government institutions handle personal information, based on my findings.

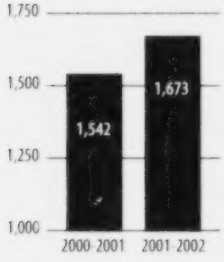
As well, I have a mandate to conduct periodic audits of federal institutions to determine their compliance with the *Act* and, on the basis of my findings, I can recommend changes.

The *Act* requires me to submit an Annual Report to Parliament on the activities of my Office in the previous fiscal year. This current report covers the period from April 1, 2001 to March 31, 2002 for the *Privacy Act*.

Investigations

My Investigations Branch investigates individuals' complaints under section 29 of the *Privacy Act* (and under section 11 of the *Personal Information Protection and Electronic Documents Act*, which I will discuss later in the report).

Complaint Investigations Closed
April 1, 2001 to March 31, 2002



Through these investigations, I determine whether individuals' privacy rights have been violated or whether they've been properly accorded access to their personal information. Where people's privacy rights have been violated, I look for ways to provide redress for them and to prevent violations from happening again.

I have authority under the *Act* to administer oaths, receive evidence and enter premises where appropriate. I can also examine or obtain copies of records found on any premises.

To date, we have had voluntary co-operation and all complaints under the *Privacy Act* have been resolved without our having to use these formal investigative powers.

Complaints under the *Privacy Act*

During the fiscal year of April 1, 2001 to March 31, 2002, we received a total of 1,213 complaints under the *Privacy Act*. Of those, 45 per cent concerned denial of access to personal information, 20 per cent were related to issues of collection, use, disclosure, retention and disposal of personal information, and the remaining 35 per cent concerned failure to respond to an access request within the legislated timeframes set out in the *Act*.

Investigations staff completed investigations of 1,673 complaints, an increase of 8 per cent over the previous year. Of those, 703 dealt with denial of access, 397 concerned issues related to collection, use, disclosure, retention and disposal of personal information, 571 were about lack of timeliness in responding to requests to obtain access to personal information and two dealt with other matters including an allegation of retaliation against an individual for submitting an access request. These complaints were concluded as follows:

Not well-founded:	445
Well-founded:	668
Well-founded/Resolved:	91
Resolved:	26
Settled during the course of the investigation:	344
Discontinued:	99

Definitions of Findings under the *Privacy Act*

Not well-founded: A finding that a complaint is *not well-founded* means that the investigation uncovered no evidence to lead me to conclude that the Government institution violated the complainant's rights under the *Privacy Act*.

Well-founded: A finding that a complaint is *well-founded* means that the Government institution failed to respect the *Privacy Act* rights of an individual. This would also be my finding in a situation where the Government institution refuses to grant access to personal information, despite my recommendation that it be released. In such a case, my next step could be to seek a review by the Federal Court of Canada.

Well-founded/Resolved: I will find a complaint to be *well-founded/resolved* when the allegations are substantiated by the investigation and the Government institution has agreed to take corrective measures to rectify the problem.

Resolved: *Resolved* is a formal finding that reflects my role as an ombudsman. It's for those complaints where *well-founded* would be too harsh to fit what essentially is a miscommunication or misunderstanding. It means that my Office, after a full and thorough investigation, has helped negotiate a solution that satisfies all the parties.

Settled during the course of the investigation: This is not a formal finding but an acceptable means to dispose of a complaint when the investigation is completed, and the complainant is satisfied with the efforts of my Office and doesn't wish to pursue the issue any further. The complainant retains the right to request a formal finding. When that happens, the investigator re-opens the file, and submits a formal report, and I report the findings in a letter to the complainant.

Discontinued: This means that the investigation was terminated before all the allegations were fully investigated. A case may be *discontinued* for any number of reasons – for instance, the complainant may no longer be interested in pursuing the matter or cannot be located to provide additional information critical to reaching a conclusion. I don't issue a formal finding in discontinued complaints.

In my report last year, I expressed concerns that a few Government departments and agencies – most notably, Correctional Service Canada (CSC), the Department of National Defence (DND), the Canada Customs and Revenue Agency (CCRA) and Human Resources Development Canada (HRDC) – had been particularly lax in responding to access requests in a timely fashion.

There are indications that these departments and agencies are improving their turnaround times as a result of special measures they have put in place to deal with their backlogs. We received fewer time-limit complaints against these institutions this past year, with the exception of DND. This fact may indicate improved performance, or simply that they received fewer requests last year and therefore fewer dissatisfied individuals turned to my Office for assistance. Regardless, most of the time-limit complaints we investigated against CSC, DND and HRDC were deemed well-founded, a clear indication that these institutions are still not meeting their obligations under the *Privacy Act*.

Summary of Select Cases Under the *Privacy Act*

Departments accountable for information collected under contract

Despite past reminders, some departments still neglect to ensure that personal information collected under the contracts they negotiate with outside contractors is managed in accordance with the fair information principles of the *Privacy Act*.

Those principles require Government institutions that are subject to the *Act* to include provisions in contracts that:

- Define ownership of the information – that is, all information collected as part of the contract belongs to the contracting department or agency and should be turned over to it at contract end;
- Recognize individuals' rights of access to their personal information collected during the contract;
- Restrict further uses of the personal data;
- Protect the information against unauthorized disclosure;
- Establish retention and disposal criteria; and
- Ensure the department's ability to audit compliance of the contractor's management of the information collected.

In one case investigated this past year, an employee of Human Resources Development Canada (HRDC) complained that she did not receive all of her personal information gathered by an independent contractor hired by the department to conduct a workplace assessment. The employee was particularly interested in obtaining access to any mention of her by other staff in the contractor's interview notes and questionnaires.

When interviewed, the contractor admitted to destroying all the information except the report she produced for HRDC. She did this in part because she had promised confidentiality to the individuals she interviewed, indicating that their statements would not be released, and the contract signed with HRDC did not specify otherwise.

Although HRDC's policies and procedures on contracting out to third parties specify that all the provisions of the *Privacy Act* are to be respected, the contractor in this case was not aware of HRDC's obligations under the *Act* to retain the information or grant individuals access to their own information. Contractors (as well as employees conducting similar administrative investigations) must be informed that they cannot promise confidentiality and, prior to taking statements about an individual, they must inform witnesses that their statements constitute the other individual's personal information for which rights of access are provided by the *Privacy Act*. The witness then has a choice as to whether or not to provide a statement that would include information about another individual.

I concluded that the complaint was well-founded and HRDC was accountable for the work done under the contract. The contractor's failure to retain the information in essence resulted in the complainant being denied an opportunity to obtain access to her own information.

In a case against the Department of National Defence, a military officer sought my assistance in getting access to his medical records, including the notes of an independent medical specialist the department hired to provide an opinion based on his review of the complainant's medical file. When the officer submitted his access request, the department released the medical records in its file, but did not release the specialist's notes from the independent review.

When I investigated the matter, I learned that no effort had been made to get the information from the specialist. I interviewed the specialist and reviewed his notes, which clearly contained personal information about the complainant. The specialist claimed that he had not been told that the information he gathered as part of his review belonged to the department and that he should also supply a copy of all the information from his file to the department for inclusion in its records. Nevertheless, the

specialist willingly provided a copy to the department so that it could in turn release it to the complainant. The complainant was pleased to receive the information and did not request that we pursue the matter further.

These two cases serve to remind federal departments and agencies that any contracts they enter into that require the collection of personal information must also include appropriate clauses to satisfy the provisions of the *Privacy Act*. Individuals should be able to access their own information whenever it is requested.

RCMP charges fee for traffic analysis report

A British Columbia man asked the Royal Canadian Mounted Police (RCMP) for a copy of a traffic analysis report prepared following an investigation of a traffic accident in which he was involved. The report attempted to reconstruct the circumstances surrounding the accident, and the man wanted to use it to support a civil claim. When he requested a copy of this report informally from the RCMP detachment where it was prepared, he was told there was a $500 fee. He then formally requested it under the *Privacy Act* but was refused on the basis that it was exempted under section 22(1)(a) of the *Act*. Section 22(1)(a) allows an investigative body such as the RCMP to deny access to information about a lawful investigation that is less than 20 years old. In his letter of complaint, the man correctly asked how the information could be available if he paid the $500 fee but not under the *Privacy Act*, to which no fees apply.

I determined that the RCMP detachment's response to the informal request was based on an established fee schedule. When the *Privacy Act* request was received at the RCMP's Access to Information and Privacy Unit in Ottawa, it confirmed that the accident was still under investigation. The RCMP routinely refuses access to information related to ongoing investigations. The unit subsequently informed the complainant that the report was exempted in its entirety under section 22(1)(a) of the *Act*.

However, upon further inquiries, I learned that in August 2000 the RCMP had issued a bulletin to all detachments in British Columbia that no fee should be collected for these reports. This decision followed a 1998 Supreme Court of British Columbia ruling in a case against the RCMP as the municipal police force under contract to the province. The Court ruled that the fee charged by the RCMP for a traffic analysis report was in essence a tax disguised as a user fee, and therefore was without any legislative authority.

As a result of our intervention, the RCMP provided the man with his own personal information in the report, which was all he was entitled to receive under the *Privacy Act*.

DND improperly retains, uses information about pardoned convictions

I investigated complaints from two Canadian Forces members who felt their privacy had been violated when the Department of National Defence (DND) kept information on its files related to their criminal convictions and subsequently used that information to deny them employment opportunities.

In the first case, the member had been selected for a posting with a United Nations tour in the Middle East, but just prior to his departure the posting was cancelled by his base commanding officer. I learned that DND's Military Police discovered the member had been charged with impaired driving shortly before his planned departure date and had reviewed its records to determine whether the man had any other charges against him. It found seven references to other criminal offences and forwarded this information to the base commanding officer. When the commanding officer saw the record, he decided against sending the member overseas.

I determined that two of the offences should have been purged from the member's file since he had received a pardon for them. The Pardons and Clemency Division of the National Parole Board had notified DND of these pardons and of the department's requirements under the *Criminal Records Act* to segregate its records related to these offences from other criminal records in its custody. DND complied but only insofar as reference to the convictions was concerned – all the facts related to the charges that led to these two convictions remained on file.

Unfortunately, when only the reference to a conviction is removed from a record, what remains can be misleading to anyone who has access to that information. I therefore reminded DND that under the *Privacy Act* it is required to ensure that personal information used for an administrative purpose – that is, in a way that directly affects the individual to whom it relates – is accurate, up-to-date and complete.

As a result of my efforts, DND agreed to amend its policy on the retention of information about pardoned convictions to conform with both the *Privacy Act* and the *Criminal Records Act*.

In the second case, an individual obtained information that led him to believe DND used information about his convictions under the *National Defence Act* to reject his application for re-engagement in the Canadian Forces, despite the fact that he had been granted a pardon.

When I investigated the matter, I confirmed that DND had indeed used this information in its assessment of his application. I also confirmed with the Pardons and Clemency Division of the National Parole Board that it had granted a pardon to the individual but

had neglected to inform DND. I therefore asked the National Parole Board to send appropriate notifications to DND and the National Archives, the current custodian of the individual's military records, so that they could amend his records as required.

CMHC's demand for tax information inappropriate

The president of a consulting firm complained that Canada Mortgage and Housing Corporation (CMHC) had asked for an excessive amount of personal information from sole proprietors and partnerships as proponents in a Request for Proposal (RFP) process. If the lead proponent turned out to be a sole proprietor, that individual was required to provide, among other things, copies of his/her income tax returns for the last three years and a statement of net worth.

I discussed the RFP process with CMHC in depth. It was adamant that it was necessary to obtain financial information from a lead proponent when there was a high degree of risk associated with procurement and that it must ask for detailed information from a sole proprietor just as it did with any other type of business. It argued that, for a sole proprietor, unlike for a corporation, there was little comprehensive financial information that could be used to conduct an accurate risk assessment and that the information it was requesting was the best and most accurate it could get.

I agreed that the financial viability of a lead proponent had to be assessed to minimize the organization's exposure in high-risk cases. However, I did not understand how this objective was achieved by assessing income tax information for a three-year period. An individual may have had substantial revenue over three years but income tax information would not reveal how the individual disposed of that revenue. A proprietor may have had three difficult years but could still support the financial strains of a contract. An individual may also have substantial assets in property or non-interest bearing investments that are simply not reflected in income tax documents.

Section 4 of the *Privacy Act* provides that personal information collected by a Government institution must relate directly to an operating program or activity of the institution. Because I did not believe that income tax information was of material assistance in helping CMHC to assess the quality of a sole proprietor's RFP proposal, I could not conclude that CMHC's request for that information met the requirements of section 4. As a result of my investigation, CMHC has amended its procurement policy and has discontinued the practice of requesting income tax returns and statements of net worth from sole proprietors.

It is unacceptable to me that Canadian citizens should have to provide copies of their personal income tax returns to do business with the Government. Under the *Income Tax Act*,

individuals must divulge a vast amount of personal information when completing their income tax returns, including a good deal of personal information about family members. The income tax process is extraordinarily intrusive and the use of personal information collected for income tax purposes must, in my view, be strictly confined to purposes that are regulated. At a time when Canadians are increasingly concerned about the erosion of their personal privacy, I find it untenable that an income tax return can be demanded from an individual for a purpose other than that required by law. Canadians should never be required to compromise a fundamental right in order to do business with the Government.

Ultimately, CMHC agreed with my finding and halted the practice. Although my investigation focused on CMHC practices, I was aware that other federal Government departments and agencies followed similar practices. I therefore wrote to the Deputy Minister for Public Works and Government Services Canada, and to the Secretary of the Treasury Board and the Comptroller General of Canada, seeking their assistance to ensure that this practice is discontinued throughout the federal Government. The Treasury Board agreed with my view. It indicated that the practice was not Government policy and that the matter would be raised with other departments and agencies. I have also been informed by Public Works and Government Services that it will discontinue the practice.

Inappropriate monitoring of employees' e-mail accounts

I investigated several complaints from individuals questioning managers' authority to search Government e-mail accounts during the course of administrative investigations.

In one instance, two employees at the Immigration and Refugee Board (IRB) alleged that local management improperly retrieved copies of confidential e-mail messages they had written each other regarding a *Privacy Act* complaint to this Office by one of the employees.

By way of background, one of the employees had discovered performance evaluations about several of her co-workers on the local computer network and immediately notified her union's representative, another IRB employee. The representative obtained copies of the evaluations to support his complaint to this Office about the improper disclosure of personal information.

My investigation of that complaint determined that the IRB had not taken adequate steps to restrict access to the information and I concluded that the complaint was well-founded.

Management of the IRB fixed the computer glitch that had created the problem as soon as it was notified of the substance of this complaint. Management also initiated an inquiry

into the incident to establish whether any disciplinary action should be taken against the employee for disclosing the evaluations to the union representative. On instruction, the local information technology manager searched and retrieved some e-mail communications concerning the incident between the employee and the union representative.

The IRB did not have a formal policy on the use of electronic networks at the time of this incident. In the absence of a policy, it is guided by Treasury Board policies dealing with employees' expectation of privacy and the statement of authorized uses. The IRB stated that it supports the principle that access to an employee's e-mail without consent is justified only in extreme situations, for example in situations involving a criminal or security infraction, and only after proper authorization from senior management.

However, in the case in question, prior to conducting the search of the electronic system, the IRB was already well aware of the employee's actions and her contact with the union representative. Its decision to retrieve their e-mail messages was not based on any concern that they were improperly using the system. Rather, the primary purpose was to conduct an internal disciplinary inquiry.

My view was that it was unnecessary for the IRB to retrieve the e-mail exchanges to determine if disciplinary action against the employee was warranted and therefore its actions could not be justified under the *Privacy Act*. I recommended that the IRB proceed quickly to complete its disciplinary review and that it publish a policy, similar to Treasury Board's, governing the use of its electronic networks.

In another case, a Human Resources Development Canada (HRDC) employee complained that her supervisor retrieved personal e-mails she sent from her home to a co-worker and improperly used them in the course of an internal investigation into allegations that had been made against her by her union local.

I established that HRDC's local management was investigating an allegation that the employee interfered with a grievance process. During the investigation HRDC searched its Internet network database for any e-mail exchanges she might have had with a particular co-worker about the grievance. HRDC made no effort to obtain the consent of either individual before searching the co-worker's office e-mail account. One personal message from the complainant to the co-worker contained a reference to the grievor by name but nothing else related to the grievance. The message was otherwise predominantly personal in nature. Yet the department subsequently used it during its investigation process.

I accept that there may be occasions that would justify an employer's decision to review an employee's Internet network account and then use that information in a disciplinary process. However, this was not such an occasion. There was no evidence to suspect that the co-worker was in any way implicated in the internal investigation that would lead HRDC to search her account. By collecting the complainant's personal e-mail exchanges with the co-worker without consent, and subsequently using it to investigate the complainant, HRDC violated her *Privacy Act* rights.

Man denied access to his information following war crimes investigation

A European immigrant, now a Canadian citizen, requested my intervention after the Royal Canadian Mounted Police (RCMP) repeatedly denied him access to its investigation file of his involvement in Nazi activities in Jewish death camps during World War II.

The man was denied entry into the United States in 1990 when his name appeared in a database containing information gathered by the U.S. Justice Department's Office of Special Investigations (OSI). The database contained the names of all members of a Nazi unit, regardless of rank, occupation or activity. The OSI then asked the RCMP to investigate the extent of the man's involvement in the Nazi unit. During the investigation, carried out jointly by the RCMP's War Crimes Section and Justice Canada's Crimes Against Humanity and War Crimes Section, the RCMP interviewed the man about the U.S. allegations.

Over a period of several years, he attempted to obtain information from the RCMP about its investigation so that he could take appropriate action to clear his name, but was always rebuffed. The RCMP claimed it was still looking into the allegations and releasing anything from its files might jeopardize the integrity of its investigation.

He requested a copy of the file again in 2000 after he received correspondence from the Department of Justice advising him that its joint investigation with the RCMP was concluded and the file had been closed. The RCMP refused again, saying the file was exempted in its entirety under section 22(1)(a) of the *Privacy Act*, and verbally told him that the case was still ongoing. He then complained to my Office.

When a privacy officer of my Investigations Branch reviewed the information withheld by the RCMP, he noted that some of the information was almost 60 years old and therefore did not qualify for exemption under the provision cited by the RCMP. The RCMP then considered applying another exempting provision, section 22(1)(b), but to do so properly, the RCMP would have to demonstrate the injury that would likely occur to its investigation if the information were released.

Since the investigation was already concluded, the privacy officer questioned how disclosure of the information could cause injury. The RCMP maintained that its investigation was not yet finalized even though there had been no activity on the file since 1997.

After the privacy officer confirmed with the Department of Justice's Crimes Against Humanity and War Crimes Section that the case was closed for lack of evidence to proceed, the RCMP conceded and agreed to disclose information from its file.

Disclosure of information during appeal should be limited

Several individuals who had appealed a Human Resources Development Canada (HRDC) decision to recoup an overpayment of employment insurance (EI) benefits, complained that personal information was improperly disclosed during the appeal process.

The complainants were among over 200 individuals who received EI benefits after losing their employment. Because they filed a grievance about their termination that resulted in being awarded severance packages, HRDC commenced action to recoup the EI benefits the individuals received for the period they were covered by the severance package. They appealed HRDC's decision to the EI Board of Referees.

As part of the appeal process, HRDC's local office sent a disclosure package to each of the appellants. Each package was to contain information related to that particular individual's appeal. However, one complainant's package included a document that contained the names, addresses, phone numbers and Social Insurance Numbers (SINs) of 14 other individuals involved in the appeal. When he informed HRDC of the impropriety, it reviewed its records and established that only two of the appellants had received this document.

HRDC immediately took steps to retrieve the document from both individuals and replace it with a properly vetted copy. It also contacted by phone or letter the others whose personal information had been inadvertently revealed and explained the error.

After they lost their appeal, the appellants sought a second-level review that required HRDC's district office to send each appellant a disclosure package related to that particular individual. Once again, one of the complainants got the identical document he had received previously, disclosing personal information about 14 other appellants. It was this second disclosure that prompted the complaint to me.

I was troubled that HRDC's district office would disclose the same information as the local office, despite the admission that the disclosure had been made in error. Clearly, the document should have been properly vetted by the local office the first time it was sent. The district office compounded this error when it sent the same information a second time, which it felt was required to ensure procedural fairness. I concluded that HRDC had violated the complainants' rights under the *Privacy Act*.

I therefore recommended that HRDC build in procedures that would respect procedural fairness throughout the various levels of the EI appeals process while at the same time recognizing its obligations under the *Privacy Act* to disclose personal information only when it is directly relevant to the appeal at hand.

In another case, a woman complained that information she had provided to HRDC to support her claim for a survivor's benefit under the *Canada Pension Plan* was disclosed to family members of her deceased common-law husband. HRDC had received applications from both the complainant and the deceased's wife by marriage, and ultimately gave the benefit to the common-law wife. The legal wife filed an appeal of HRDC's decision with the Office of the Commissioner of the Review Tribunals (OCRT).

The *Review Tribunal Rules of Procedure* require HRDC to convey to the OCRT copies of any documents relevant to its decisions. Under the same *Rules*, the OCRT must share copies of these same documents with the appellant. Therefore, the OCRT provided copies of all documents it received from the deceased's common-law wife. These documents contained information the common-law wife had given to HRDC to demonstrate her relationship with the deceased and her entitlement to the benefit – including her SIN, her application for Old Age Security, a copy of a property deed and information about a joint bank account.

HRDC's disclosure to the OCRT does not offend the *Privacy Act* – it was in accordance with a regulation that authorized the disclosure under an Act of Parliament. Furthermore, the OCRT is not subject to the *Privacy Act*. Nevertheless, I was concerned that the OCRT obtained more information from HRDC than was absolutely required. Some information, such as the common-law wife's SIN and details about her bank account, was not necessarily a factor in HRDC's decision, and did not need to be shared with the OCRT for appeal purposes. In response to my concerns, HRDC agreed to review the documents it intends to submit to the OCRT on a case-by-case basis, keeping in mind the privacy rights of all individuals concerned while providing sufficient information to ensure a fair and complete hearing.

Canada Post changes stance on using negative consent to sell addresses to mass mailers

My Office received a complaint that Canada Post, a Crown corporation, was improperly disclosing personal information collected for its National Change of Address (NCOA) service. The complainant stated that Canada Post was selling subscribers' new addresses to mass mailers and direct-marketing companies unless subscribers to the service contacted the corporation in writing to specifically request that their information not be used for that purpose. This practice is what is known as "negative consent," and it is something Canadians have been known to get very upset about.

For this service, individuals pay a fee to Canada Post to have their mail forwarded until they have had an opportunity to notify others of their change of address. To subscribe, they sign a Change of Address Notification (COAN) form containing the following acknowledgement:

> … I understand the information I provide will be used to deliver mail to my new address. I also agree Canada Post may supply this new address to mailers, provided they request it and already have my correct name(s) and old address.

By signing this statement, individuals asked Canada Post to perform the specific service they paid for – redirecting their mail to their new address. But they were also agreeing to something that they didn't specifically request – allowing Canada Post to sell their new address to mass mailers and direct-marketing companies – unless, as indicated on the back of the form, they wrote in and told the corporation not to do so within seven days.

Many individuals may have read this section, without realizing that "supply" meant sell and that "mailers" meant *any* mailers – primarily, companies that send junk mail.

I informed Canada Post of my concern that subscribers were not aware they were consenting to the provision of their information to mass mailers when they signed the COAN form. Canada Post argued that subscribers provided consent when they signed the form and that they could notify the corporation if they did not want their new address provided to all mailers. I pointed out that, to stop Canada Post from selling their information to mass mailers, subscribers would have to read the fine print on the front of the form that referred them to further details on the reverse side. The reverse side stated the following: "At no additional cost, Canada Post will help you advise businesses and other organizations of your new permanent address."

I disagreed with Canada Post's stance that it had obtained consent. Not only is the notion of "negative consent" insensitive to the privacy rights of Canadians, but Canada Post didn't really obtain proper consent at all. Under the *Privacy Act*, an organization does not have your consent if it has not told you what you are consenting to.

Informed consent was the real issue. Section 5(2) of the *Act* requires a Government institution to inform you of its purposes when it collects personal information from you. Was Canada Post informing those who subscribed to the NCOA service of its purposes, plainly and fully? Would reasonable persons, on reading the COAN form, conclude that they were giving consent for the sale of their personal information to mass mailers and direct marketers? I was quite sure they would not. In matters involving consent, the reasonable expectations of the individual are also relevant.

Canada Post initially agreed to adopt some of my recommendations to make the NCOA service more transparent and sensitive to privacy rights. It agreed to replace the word "acknowledgment" with "authorization" on the front of the COAN form and to add the phrase "including direct mailers" in the statement. But Canada Post was reluctant to accept my main recommendation: to give subscribers to the service a positive choice in the matter by adding an opt-in box on the front of the form. It believed that such an addition risked undermining the NCOA service and would lead to frustration and inconvenience for its customers.

I convinced Canada Post otherwise. I argued that Canada Post would benefit from such an addition, since its customers would appreciate that the corporation was doing everything in its power to maintain their privacy, and that customers would also benefit. Customers who want to receive mail from mass mailers can clearly indicate their choice, while those who don't want the junk mail will also have a choice in the matter. But the customer would have the choice, not Canada Post.

Canada Post finally agreed to add an opt-in box on its COAN form.

Incidents under the *Privacy Act*

The Investigations Branch staff makes inquiries about incidents that have come to my attention from various sources, but are not considered to be formal complaints under the *Privacy Act*. Many of these incidents concern the management (or mismanagement) of personal information – inadvertent disclosures to third parties, or lost or stolen files and electronic notebooks. Some examples follow.

Improper disclosure of SIN on Canada Child Tax Benefit forms

In one case, a newspaper reported that the Canada Customs and Revenue Agency (CCRA) had accidentally released information about individuals in western Canada in receipt of a Canada Child Tax Benefit (CCTB). When we looked into the matter, we learned that some taxpayers received page one and two of their own Notice of Determination form and page three containing information about another taxpayer. The information on page three displayed the taxpayer's Social Insurance Number (SIN), first name of the spouse where applicable, and the payment schedule for the year.

Even though the taxpayer's name is not displayed, the Social Insurance Number is a unique number assigned to that taxpayer and therefore constitutes personal information as defined by the *Privacy Act*. Fortunately, and contrary to the media report, the information did not include the other taxpayer's surname, home address, children's names or their dates of birth, or family income. Nevertheless, we've all heard stories about the results of SINs getting into the wrong hands and the havoc that this can wreak on a person's life.

CCRA also conducted its own investigation and determined that the problem was the result of a printing synchronization error, probably because of a computer glitch. To prevent a similar problem from occurring in the future, CCRA has enhanced its systems to detect any malfunction of the printer's sorting function and shut it down. Operator intervention will be required to continue the print job after appropriate inspection has been carried out. As a result of this incident, CCRA has decided that it is no longer necessary to print the Social Insurance Number on the second and any subsequent pages of the CCTB Notice of Determination form.

Gun registry documents found in dumpster

Several days before Christmas, a man called my Office to report that he had found three bags containing personal information belonging to the Canadian Firearms Program in a dumpster in a locked compound owned by the private company where he worked.

My investigators went to the scene immediately. The location was not anywhere near the Canadian Firearms Program processing site, and the dumpster was strictly used for wood products. My investigators retrieved a number of envelopes addressed to the Canadian Firearms Program, most of which contained names and return addresses of individuals.

My investigators then confirmed that, during the fall, the Canadian Firearms Program had sent packages containing personalized applications to all firearms owners, along with return envelopes pre-addressed to the Canadian Firearms Program. The information they found in the dumpster contained the pre-addressed envelopes that had been returned to the Canadian Firearms Program.

Having established that the information originated from the Canadian Firearms Program, my investigators tried to determine how it had ended up in the compound of a private company. They confirmed that the dumpster was rented by a waste management company and had been in the compound since early December.

My investigators observed that the bags found in the dumpster were covered in snow and were stuck to the bottom of the dumpster. It is likely that when the waste company retrieved the dumpster from a previous location and emptied it, the bags stayed within.

My officials contacted the Department of Justice, the Government institution responsible for the gun registration program. Officials stated that the department had contracted out the processing of the registration forms to a private company. The company is fully cognizant of the provisions of the *Privacy Act* and thought it had taken every precaution to safeguard individuals' privacy rights. However, company officials confirmed that the normal practice was to throw out the pre-addressed return envelopes using a regular garbage can, without realizing that firearms owners had written their names and return addresses on the envelopes, which would make them easily identifiable as firearms owners. The company agreed to immediately stop throwing the envelopes into the regular garbage and undertook to dispose of them in a secure manner, through shredding.

HRDC/CCRA to share data on eligibility for Guaranteed Income Supplement

I took a special interest in another situation that received a great deal of media attention – the apparent inability of the Canada Customs and Revenue Agency (CCRA) to share information with Human Resources Development Canada (HRDC) that would identify senior citizens who are eligible to receive the Guaranteed Income Supplement (GIS). The GIS is a component of the Old Age Security (OAS) benefit and is granted to those seniors in the lower income bracket. Approximately 1.5 million seniors receive the GIS. Although this case did not directly involve the *Privacy Act*, I did not want privacy legislation or my Office to be seen as a barrier preventing federal Government departments from engaging in activities that benefit Canadians.

CCRA has taxpayer information that would reveal which seniors would qualify to receive the supplement, but it refused to share their identities with HRDC's Income Security Programs Branch that grants the benefit because of the confidentiality provisions of the *Income Tax Act*. In my view, the *Income Tax Act* contains specific authorization to disclose personal information for the purpose of administering the *Old Age Security Act*, as I testified before a House of Commons committee on the matter.

Following media reports about the lack of cooperation between the two arms of Government, my Office met with officials of HRDC and CCRA to facilitate a solution to the problem, and to help ensure that seniors who qualify for the GIS are made aware of the availability of the income supplement. As a result of these efforts:

- CCRA added a page for lower income seniors to its 2001 tax guide with key messages about the GIS and how to apply;
- CCRA will send information about OAS and GIS benefits to people over age 65 who have a low or modest income; and
- HRDC will receive from CCRA a list of low-income seniors who receive the OAS benefit but not the GIS. Using income data supplied by CCRA and existing personal data from the OAS application form, HRDC will provide potential GIS clients with a simplified GIS application form containing their pre-printed name, address and income information. It will ask them to confirm or correct the information on the form so that their eligibility for GIS benefits can be decided upon return of the form to HRDC.

I understand that both HRDC and CCRA recognize the need for a more streamlined process that ensures the legal underpinnings are in place to make seniors aware of their entitlement to benefits. My staff and I are available to both departments to discuss other initiatives and to provide whatever assistance we can to ensure that there are no adverse implications from a privacy perspective.

Public Interest Disclosures

Paragraph 8(2)(m) of the *Privacy Act* allows the head of a Government institution to disclose personal information in the public interest, without the individual's express consent – either because disclosure clearly outweighs any consequential invasion of

privacy that might result, or because it would benefit the individual to whom the information relates. This provision is designed to deal with those situations where the Government institution cannot satisfy any other provision set out in subsection 8(2) of the *Act* to justify the disclosure. Subsection 8(5) of the *Act* imposes a mandatory duty on the heads of Government institutions to notify the Privacy Commissioner in writing of any public interest disclosure of personal information. The notice is to be issued in advance unless the situation requiring disclosure is so urgent and pressing that failure to act immediately would itself contribute to some identifiable harm.

This past year, I reviewed 57 notifications that personal information would be disclosed in the public interest. Almost one half of these were generated by Correctional Service Canada (CSC). CSC receives requests from third parties, including victims groups, for Board of Inquiry reports dealing with issues that have often received wide media attention, including prison escapes and violent criminal activities of offenders still under CSC supervision. It also receives requests for information from family members of offenders who died while under CSC supervision. The public interest disclosure provision of the *Privacy Act* is CSC's only authority to release personal information to the family on compassionate grounds, so that the family can have a better understanding of what happened and to help them achieve some degree of closure.

I also reviewed the circumstances related to a notification to me from the RCMP that it intended to release personal information about a convicted criminal to the media. The information requested by the media related to a videotape that had been entered into evidence in the offender's trial, which the media had wanted to use in an exposé about the criminal's highly publicized case. The media had turned to the RCMP for assistance after discovering that the Court had destroyed its copy of the tape – the Court does not retain indefinitely all evidence or exhibits presented during proceedings. The only existing copy was in the possession of the RCMP.

I failed to see how the public interest would be served by disclosing the information under these circumstances and asked the RCMP to reconsider its position. Although the tape was used as evidence in a criminal proceeding, which is public in nature, it is first and foremost personal information about an identifiable individual contained in the RCMP's investigative records, which are not generally publicly available. I therefore recommended to the RCMP that it refuse to disclose the tape. The RCMP complied with my recommendation.

Top Ten Departments by Complaints Received

April 1, 2001 to March 31, 2002

Organization	Total	Access to Personal Information	Time	Privacy	Other
Canada Customs and Revenue Agency	307	152	85	69	1
Correctional Service Canada	265	84	125	56	0
Human Resources Development Canada	117	42	57	18	0
Citizenship and Immigration Canada	103	57	40	6	0
Royal Canadian Mounted Police	89	65	16	8	0
National Defence	78	31	35	11	1
Immigration and Refugee Board of Canada	41	6	29	6	0
Canada Post Corporation	32	12	6	14	0
Justice Canada	22	6	5	11	0
Canadian Security Intelligence Service	18	18	0	0	0
Others	141	67	30	44	0
Total	**1,213**	**540**	**428**	**243**	**2**

Completed Investigations and Results by Department

April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Agriculture and Agri-Food Canada	0	0	1	1	0	0	2
Atlantic Canada Opportunities Agency	0	0	0	0	0	2	2
Bank of Canada	0	0	0	0	0	3	3
Canada Customs and Revenue Agency	44	20	120	8	10	63	265
Canada Mortgage and Housing Corporation	1	0	0	0	0	0	1
Canada Post Corporation	5	7	10	2	2	16	42
Canadian Environmental Assessment Agency	0	0	2	0	0	0	2
Canadian Grain Commission	0	1	0	0	0	2	3
Canadian Heritage	0	0	1	0	0	1	2
Canadian Human Rights Commission	0	0	2	0	0	1	3
Canadian Museum of Civilization Corporation	1	0	0	0	0	0	1
Canadian Nuclear Safety Commission	0	0	0	0	0	3	3
Canadian Radio-Television and Telecommunications Commission	0	0	1	0	0	1	2
Canadian Security Intelligence Service	0	0	35	1	0	1	37
Canadian Space Agency	3	1	1	1	0	0	6
Citizenship and Immigration Canada	40	4	26	11	0	17	98

Completed Investigations and Results by Department (Continued)
April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Commission for Public Complaints against the RCMP	1	2	4	0	0	1	8
Correctional Investigator Canada	1	0	0	0	0	0	1
Correctional Service Canada	344	11	47	17	1	89	509
Environment Canada	2	0	1	0	0	1	4
Farm Credit Canada	0	3	1	0	0	1	5
Fisheries and Oceans Canada	0	0	1	0	0	0	1
Foreign Affairs and International Trade Canada	24	0	4	0	0	1	29
Health Canada	0	0	0	2	0	4	6
Human Resources Development Canada	86	10	45	24	2	36	203
Immigration and Refugee Board	29	1	3	0	0	6	39
Indian and Northern Affairs Canada	1	1	9	1	1	0	13
Industry Canada	1	0	4	1	1	2	9
Justice Canada	8	1	12	4	1	8	34
National Archives of Canada	1	0	3	1	0	5	10
National Defence	44	14	20	8	3	25	114
National Gallery of Canada	0	0	0	0	0	1	1
National Parole Board	0	3	9	3	0	5	20
Natural Resources Canada	0	0	1	0	0	1	2
Office of the Chief Electoral Officer	0	1	1	0	1	2	5

Completed Investigations and Results by Department (Continued)
April 1, 2001 to March 31, 2002

Organization	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Office of the Commissioner of Official Languages	0	0	0	1	0	0	1
Office of the Superintendent of Financial Institutions	0	0	1	0	0	0	1
Ombudsman National Defence and Canadian Forces	1	0	1	0	0	0	2
Privy Council Office	3	1	0	0	0	0	4
Public Service Commission of Canada	1	2	0	0	0	2	5
Public Service Staff Relations Board	0	0	1	0	0	0	1
Public Works and Government Services Canada	1	0	1	2	0	6	10
Royal Canadian Mounted Police	20	6	66	10	3	36	141
Solicitor General Canada	2	0	2	0	0	0	4
Statistics Canada	3	0	2	0	0	0	5
Status of Women Canada	0	0	2	0	0	0	2
Toronto Port Authority	1	0	0	0	0	0	1
Transport Canada	0	2	1	0	0	0	3
Treasury Board of Canada Secretariat	0	0	3	0	0	0	3
Veterans Affairs Canada	0	0	1	1	1	1	4
Western Economic Diversification Canada	0	0	0	0	0	1	1
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1,673**

Completed Investigations by Grounds and Results

April 1, 2001 to March 31, 2002

	Well-founded	Well-founded/ Resolved	Not Well-founded	Discontinued	Resolved	Settled	Total
Access to Personal Information	**22**	**80**	**260**	**60**	**22**	**259**	**703**
Access	22	77	249	53	22	248	671
Correction/Notation	0	3	9	4	0	4	20
Language	0	0	1	3	0	4	8
Inappropriate Fees	0	0	1	0	0	3	4
Privacy	**184**	**11**	**99**	**26**	**4**	**73**	**397**
Collection	10	2	26	2	0	19	59
Retention and Disposal	10	2	5	1	1	7	26
Use and Disclosure	164	7	68	23	3	47	312
Time Limits	**462**	**0**	**85**	**13**	**0**	**11**	**571**
Correction/Time	4	0	0	1	0	1	6
Time Limits	440	0	53	9	0	9	511
Extension Notice	18	0	32	3	0	1	54
Other	**0**	**0**	**1**	**0**	**0**	**1**	**2**
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1,673**

Origin of Completed Investigations
April 1, 2001 to March 31, 2002

Province/Territory	Number
Newfoundland	3
Prince Edward Island	4
Nova Scotia	57
New Brunswick	60
Quebec	257
National Capital Region–Quebec	11
National Capital Region–Ontario	116
Ontario	433
Manitoba	92
Saskatchewan	39
Alberta	271
British Columbia	315
Nunavut	0
Northwest Territories	0
Yukon	5
International	10
Total	**1,673**

Privacy Practices and Reviews

Introduction

Section 37 of the *Privacy Act* permits me to initiate compliance reviews, at random, of the personal information-handling practices of federal institutions. What this means is that I audit them, to verify whether they are complying with the principles for the collection, use, disclosure, protection, retention and disposal of personal information set out in sections 4 to 8 of the *Act*.

The Office has been conducting compliance reviews under section 37 since 1984. I have expanded this function during the past year, setting up a Privacy Practices and Reviews Branch, to allow me to assess how well organizations are complying with the requirements set out in the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*. (The private sector legislation gives me similar powers of audit; my discussion of private sector audit activity is in Part Two of this Report.)

As an ombudsman, I want privacy audits to be non-confrontational whenever possible. An audit, ideally, is a co-operative, constructive approach to dealing with issues before they become complaints. It's useful for organizations that want to improve their personal information-handling practices. Although I have the same powers with respect to audits that I do in investigations – to summon witnesses, administer oaths, and compel organizations to produce evidence – I would only resort to them if I didn't get voluntary co-operation.

My staff in the Privacy Practices and Reviews Branch, in addition to auditing and reviewing, works with federal organizations that are looking for a better understanding of compliance issues and the privacy implications of programs and practices. It's critical for Government departments to fully explore how privacy can be protected before they go ahead with plans, however well intentioned, to cut costs or protect citizens. On request, my branch staff reviews new proposals for information management, such as data-matching initiatives, the creation of databases and information-sharing arrangements with other organizations. This is another way to help ensure that Canadians' privacy rights are respected.

In the past year, my Office completed reviews of the personal information-handling practices under section 37 of the *Privacy Act* at the Canadian Nuclear Safety Commission (CNSC) and the Immigration and Refugee Board (IRB).

The objectives of the reviews were: to learn where and how the CNSC and the IRB handle personal information; to determine the degree to which their personal information management policies and practices are in compliance with sections 4 to 8 of the *Privacy*

Act in terms of the principles of fair information practices; and to offer observations and recommendations, where necessary. At the end of each review, organizations received reports complete with detailed findings and recommendations. I have recently issued the reports of our compliance reviews to the CNSC and the IRB, and I am awaiting their responses to the findings and recommendations.

It is not my intention to routinely disclose review findings unless the issues uncovered are so outstanding as to warrant public disclosure. An outstanding issue presented itself in the review of the IRB.

The review revealed that the Montreal, Vancouver and Toronto regional offices use closed circuit television equipment to monitor public reception and waiting rooms, as well as in hallways adjacent to hearing rooms. In some cases, video and audio equipment was installed inside hearing rooms. At the time of the compliance review, IRB did not have internal written policies or procedures regarding the use of electronic surveillance equipment, and no signage existed to inform individuals that they may be under surveillance in the areas where such devices are used.

My Office was particularly concerned about the existence of secret microphones in hearing rooms at the Montreal regional office of which headquarters were unaware. The conduct of covert surveillance – whether it involves the use of video surveillance equipment or other recording devices – is a major infringement of an individual's right to privacy and must be properly justified. No reasonable justification was provided concerning the installation of such equipment. IRB officials have since confirmed that the microphones in question have been dismantled and they assert that the listening devices were never used. My Office was also informed that the unions have been advised of the matter and that the IRB has developed a security policy requiring all regions to submit their security plans to headquarters for approval before implementation.

Update on Canadian Firearms Program

Since the mid-1990s my Office has taken a keen interest in the Canadian Firearms Program. The *Firearms Act* is a highly controversial piece of legislation that continues to produce strong emotions among both its supporters and its critics. My continued interest in the implementation of this legislation is simple: the Firearms Program involves the collection and use of a large amount of highly sensitive personal information. This legislation also has a direct impact on more than 2.3 million firearm owners, involving more than 7 million firearms in Canada. I also continue to receive complaints and inquiries about various aspects of the program, including some from Members of Parliament.

On August 29, 2001, I issued my report entitled *Review of the Personal Information Handling Practices of the Canadian Firearms Program* to the Department of Justice and the RCMP. Part 1 of the report summarized my Office's review of the program's compliance with sections 4 to 8 of the *Privacy Act* dealing with the handling of personal information. Part 2 contained our assessment of the pertinence of questions about personal history used on the firearms licence applications and their compliance with the *Privacy Act*. The report contained some 34 detailed recommendations for corrective measures aimed at reducing the intrusiveness of the program.

None of my recommendations to the Department of Justice has yet been accepted. The RCMP, however, has agreed to implement some of the recommendations from my report. I am pleased to note, for instance, that firearms officers across Canada no longer have full query access privileges to the RCMP's Police Information Retrieval System (PIRS) and that all of my recommendations with respect to limiting the use of PIRS have been implemented. In addition, I expect that the RCMP will complete the necessary revisions to the Memoranda of Understanding regarding four informatics and security areas related to the Firearms Program in the near future. These important steps will help to tighten up the control of access to sensitive personal information used in the program.

While I do not have the power under the *Privacy Act* to force the department to implement my recommendations, I will continue my efforts to urge the department to take appropriate measures to bring the Canadian Firearms Program into full compliance with the *Act*.

Subsequent to the research and fieldwork that formed the basis of my original report, other issues came to light. My Office has been monitoring the following outstanding issues:

- Outsourcing – Implementation of the existing contractual arrangement with BDP Business Data Services Ltd., all aspects of the Alternative Service Delivery initiative, as well as the current practice of outsourcing secondary and tertiary screening functions; and
- Any international information-sharing arrangements relating to the Canadian Firearms Program, whether directly or indirectly through other enforcement agencies.

Update on HRDC Governance protocol for the Databank Review Committee

In last year's Annual Report, I described how, under mounting public pressure, Human Resources Development Canada (HRDC) made the decision to dismantle the Longitudinal Labour Force File and implement a review process and a governance protocol for all policy analysis, research and evaluation activities involving the connection of separate databanks. As I explained then, this review process would involve consultation with my Office to examine such projects.

Since the last reporting period, my Office has provided comments on an additional 17 HRDC submissions, including the Review of the Action Centre for Employment, the Non-Experimental Evaluation of Investigation and Control, and the Testing of Probabilistic Record Linkage projects, to name a few. I thought it appropriate to discuss some examples of the work that we have done over the course of the year in terms of reviewing and providing comments in relation to these submissions.

My Office developed a customized assessment tool to provide a timely review of the HRDC submissions. The tool is intended to ensure that the review of such projects is consistently thorough and that all the principles of fair information practices in the *Privacy Act* are respected in the submissions. Although we are still testing its efficacy, my Office has had positive results using the tool to date.

By reviewing the development of HRDC's research projects, my Office's involvement serves as a critical check to protect privacy and often raises broader questions in relation to the use of personal information for purposes related to research and evaluation.

For instance, the Non-Experimental Evaluation of Investigation and Control (I&C) program sought to identify savings and determine the extent of deterrence resulting from I&C activities as a way of evaluating the short-term impact of the I&C function and better managing the branch. To accomplish this, HRDC research officers linked EI claim data with I&C case files and, using specific statistical methods, estimated the likelihood of EI fraud based on basic characteristics such as demographics, industry and other variables. Based on this analysis, HRDC researchers produced an equation that could be used to estimate the likelihood of EI fraud for other EI claims and therefore to evaluate the effectiveness of I&C interventions.

Although the objectives of the evaluation project were detailed and HRDC had the authority to evaluate the program, the submission was unclear with respect to the subsequent use of this equation following completion of the evaluation project. My

Office was concerned that, although it was created in the context of research, HRDC could eventually use such an equation to make decisions directly affecting individuals, such as by systematically profiling all EI claims for potential investigations solely based on the results of the equation. Since access to the personal information was strictly for research and evaluation purposes, my Office was of the view that I&C could not use the equation for administrative or enforcement purposes directly affecting a particular individual.

My Office clarified this issue with HRDC, which confirmed that it never intended to use the equation for operational purposes and, specifically, that it would not use the method to profile individuals for investigation. HRDC effectively established a clear separation between its research work and its enforcement branch. Although it is clear that HRDC had implemented the appropriate practices in relation to this project, the example serves to illustrate that use of personal information for "research or evaluation purposes" can have potential pitfalls if left unchecked.

It is worth noting that my Office has noticed a marked improvement in the level of detail and completeness of HRDC's project submissions in terms of addressing privacy concerns. Nevertheless, there is always room for improvement when it comes to privacy. In reviewing some of the HRDC submissions a common deficiency was noted: since many of the proposals are not yet finalized, they only provide limited information in relation to contracts involving outside parties.

Although HRDC has provided some examples of proposed contractual language, there is often little or no reference to the *Privacy Act*. My Office has insisted on the importance of protecting privacy in contractual agreements with consultants and third parties. We have clearly stipulated that all such contractual agreements must state that all personal information involved in the research is deemed to be under the control of HRDC; that such information is subject to the provisions of the *Privacy Act*; and that consultants and third parties must explicitly undertake to comply with all of the requirements of the *Act*.

The significance of this clause is two-fold. First, it holds the consultant accountable to the same standards of information management that are in place across Government and, second, it ensures that the provisions related to the conduct of reviews and investigations contained in the *Privacy Act* are applicable and enforceable. Although we have every confidence that HRDC is integrating these clauses in its contracts, it is important to remember that part of my role is to conduct reviews to determine whether the actual privacy practices of a Government organization are consistent with the fair information principles under the *Privacy Act*.

IN THE COURTS

Introduction

Section 41 of the *Privacy Act* allows an individual, following my investigation, to apply to the Federal Court of Canada for review of a Government institution's decision to refuse the individual access to his or her personal information. From the time the *Privacy Act* came into force in 1983, 118 applications for review have been filed in the Federal Court. Twelve of these were filed in the year ending March 31, 2002.

Section 42 of the *Privacy Act* allows me to appear in Federal Court. I can apply to the Federal Court for review of a Government institution's decision to refuse access to personal information if I have the consent of the individual who requested the information; appear before the Court on behalf of an individual who has applied for review under section 41; or, with leave of the Court, appear as a party to any review applied for under section 41.

The following is not an exhaustive list of all *Privacy Act* applications in the courts but rather a summary of matters in which I am actively involved:

Traveller Declaration Forms (Form E-311)

We pursued two cases based on the disclosure of personal information by Canada Customs and Revenue Agency (CCRA) to the Canada Employment Insurance Commission (CEIC) for use in an investigative data match program to determine if persons were fraudulently receiving Employment Insurance benefits while outside of Canada. The personal information in question was taken from Traveller Declaration Forms (E-311 forms) presented to Customs by Canadian residents returning to Canada between 1994 and 1996.

- *Privacy Commissioner v. Attorney General of Canada*

  The Federal Court of Appeal found that the disclosure of personal information from the E-311 forms was authorized by section 8(2)(b) of the *Privacy Act* and section 108 of the *Customs Act*, which gave the Minister of National Revenue discretion to disclose information collected by the department. In this case, the Court found the disclosure of information by the CCRA to the CEIC pursuant to an MOU governing terms and conditions of disclosure to be authorized. (Section 108 of the *Customs Act* has now been amended under Bill S-23.)

- *The Charter Challenge*

  The Federal Court of Appeal found there to be no reasonable expectation of privacy sufficient to engage section 8 of the *Canadian Charter of Rights and Freedoms* in the information contained in E-311 forms. This conclusion was based on two elements: the limited nature of the information in question, which did not reveal intimate details of the lifestyle and personal choices of the individual, and the narrow enforcement use to which the information was put.

Status

The cases were heard on November 7, 2001. The Supreme Court of Canada released its decisions in both cases on December 7, 2001. In each case, the reasoning of the Federal Court of Appeal was affirmed. In the Charter Challenge, the Supreme Court specifically concluded that there was no reasonable expectation of privacy in relation to the disclosed portion of the E-311 information which outweighed the CEIC's interest in ensuring compliance with the self-reporting obligations of the Unemployment Insurance benefit program.

Information Commissioner of Canada v. Commissioner of the RCMP and Privacy Commissioner

A list of the career postings of four named Royal Canadian Mounted Police (RCMP) officers was requested under the *Access to Information Act*. The Commissioner of the RCMP refused to release the information on grounds that it revealed employment history and thus was personal information as defined in section 3 of the *Privacy Act*.

At issue was whether the information could be disclosed under paragraph (j) of the definition of personal information in the *Privacy Act*, which states that information relating to the position or functions of Government officers or employees is not personal information. The larger question was the appropriate balance between the provisions of the *Access to Information Act* and those of the *Privacy Act*. The Federal Court of Appeal held that the information was personal information and did not fall under the paragraph (j) exception. The Court found that the exception should be construed in a way that does not allow for the disclosure of an individual's employment history.

Status

The Information Commissioner obtained leave to appeal this decision to the Supreme Court of Canada. I was granted leave to intervene in the appeal on January 7, 2002. The case was heard on October 29, 2002, after which the Court reserved its decision.

Clayton Charles Ruby v. Solicitor General

The Canadian Security Intelligence Service (CSIS) refused Mr. Ruby's request for access to his personal information. Mr. Ruby filed for a court review under section 41 of the *Privacy Act*.

During the court review, Mr. Ruby raised *Charter* concerns regarding the constitutionality of section 51 of the *Privacy Act*. This section provides for closed hearings (in camera) or hearings that exclude one party to the conflict (*ex parte*), where a Government institution has claimed the "foreign confidences" or the "national security" exemptions under the *Act*. The Federal Court of Appeal decided that these provisions (sections 51(2)(a) and 51(3) of the *Privacy Act* respectively) infringed on the freedom of the press, which is protected by section 2(b) of the *Charter*, but those provisions were justified under section 1 of the *Charter*. The provisions were found not to violate the right to life, liberty and security of the person protected by section 7 of the *Charter*.

Status

Mr. Ruby was granted leave to appeal to the Supreme Court of Canada concerning the *Charter* issue on January 18, 2001. The Solicitor General was granted leave to cross-appeal, and I was granted leave to intervene, on an issue concerning the interpretation of section 22(1)(b) of the *Privacy Act*. The case was heard by the Supreme Court of Canada on April 24, 2002 and the decision was rendered on November 21, 2002.

The Supreme Court held that the section 51 procedures in the *Privacy Act* do not fall below the level of fairness required by section 7 of the *Charter*. The Court did not find it necessary to the disposition of the case to decide on the privacy arguments raised by Mr. Ruby under section 7. Therefore, from a privacy perspective, the ruling does not affect the status quo. The mandatory *in camera* provision in section 51 does, however, contravene section 2(b) of the *Charter*. The Supreme Court further found that the provision could not be justified under section 1 of the *Charter*. The provision is unconstitutional and must be "read down" to apply only to those parts of the hearing that involve the merits of an exemption. The Supreme Court noted that the past judicial practice under section 51 was in fact to conduct the hearing in open court and to hear only the merits of the exemptions in camera.

With respect to the cross-appeal, the Supreme Court confirmed the finding it made in *Robert Lavigne v. Office of the Commissioner of Official Languages* on the interpretation of section 22(1)(b) of the *Privacy Act* (as follows).

Robert Lavigne v. Office of the Commissioner of Official Languages

Mr. Lavigne was refused access to information about himself contained in witness statements made in the course of an investigation conducted by the Office of the Commissioner of Official Languages. The office based its refusal of access on the exemption contained in section 22(1)(b) of the *Privacy Act*.

The Federal Court of Appeal held that section 22(1)(b) can only be invoked where there is evidence of injury to a specific investigation; that it cannot be invoked once the specific investigation has been completed; and that the allegation of a "chilling effect" on future investigations is not sufficient to support refusal to disclose.

Status

The Commissioner of Official Languages was granted leave to appeal to the Supreme Court of Canada on April 19, 2001. I was granted leave to intervene in support of Mr. Lavigne. The case was heard by the Supreme Court of Canada on January 17, 2002 and its decision was released on June 20, 2002.

The Supreme Court concluded that the exemption in section 22(1)(b) was not limited to current investigations. However, where an institution wishes to rely on the exemption in respect of harm to future investigations, it must be able to demonstrate a clear and direct connection between the disclosure of the information and the injury that is alleged.

The Supreme Court found that the Office of the Commissioner of Official Languages had not satisfied this test and ordered that Mr. Lavigne be given access to his personal information.

Information Commissioner of Canada v. Minister of Citizenship and Immigration Canada and Philip W. Pirie

Mr. Pirie was refused access to the identities of employees who gave views or opinions about him during an administrative review conducted by Citizenship and Immigration Canada. The information was withheld as the personal information of those employees under section 19(1) of the *Access to Information Act*.

The Federal Court Trial Division concluded that the identity of the individuals who expressed views about Mr. Pirie was their own personal information and should not be disclosed to Mr. Pirie.

Status

The Information Commissioner filed an appeal arguing that the identities of individuals who commented about Mr. Pirie during the review process are the personal information of Mr. Pirie under paragraph (g) of the definition of personal information in the *Privacy Act*. I was granted leave to intervene at the Federal Court of Appeal in support of the Information Commissioner's position. The matter was heard on June 4, 2002 and the Court's decision was released on June 21, 2002.

The Federal Court of Appeal agreed with the Information Commissioner and me that the identities of the persons interviewed should be disclosed to Mr. Pirie. The Court observed that the names of the interviewees were personal to both Mr. Pirie and to the interviewees, but that one interest must prevail over the other. The Court looked at the private and public interests at stake, and concluded that both mandated the disclosure of the names to Mr. Pirie. This decision is not being appealed to the Supreme Court.

Mertie Anne Beatty et al. v. the Chief Statistician et al.

This is a recent application brought by a group of Canadian citizens who seek access to the 1906 census returns for the provinces of Manitoba, Saskatchewan and Alberta. The applicants seek an order compelling the Chief Statistician to transfer the 1906 census returns to the National Archivist, and an order directing the National Archivist to make the returns available to the public for research purposes in accordance with section 6 of the *Privacy Regulations*.

Status

The application was filed on February 5, 2002, and I was one of the named respondents. All arguments have now been filed. A hearing date has not been set.

Part Two
Report on the *Personal Information Protection and Electronic Documents Act*

Introduction

A year is not long in the life of a law – not long enough, perhaps, to afford a basis at present for a comprehensive analysis of the application of the *Personal Information Protection and Electronic Documents (PIPED) Act.* Still, from the 28 investigations we finalized under the *PIPED Act* in 2001, I was able to draw some fairly solid conclusions on two fronts at least, and I believe it is instructive to share those conclusions at this time. (I will report on the experience with the second year of the *PIPED Act* in my upcoming next Annual Report.)

In particular, there has been considerable progress made in interpreting what is and what is not personal information, and in determining areas in which organizations typically seem to be having problems adapting to the requirements of the *Act.*

The Definition of Personal Information: Broad but not Infinite

Section 2 of the *PIPED Act* defines personal information simply as "information about an identifiable individual." That definition is meant to cover a lot of ground, and the first year of the *Act* served in good measure to clarify what ground it does, and does not, cover.

Several cases have already given rise to disputes over whether the information at issue constituted the complainant's personal information. Notably, some organizations have been quick to claim "ownership" of certain items of information assigned to customers, such as account numbers, identification numbers and credit cards. The usual argument is that such information should not be considered personal because it is not collected from customers. Because it is generated internally by the organization itself, it is deemed by corporate convention to be the organization's property.

But the section 2 definition was designed to sidestep such arguments. It doesn't say that personal information has to originate with or be collected from the individual. It doesn't concern itself with who may or may not be said to have proprietary interest in the information. It only says that information is personal if it is "about" an identifiable individual. When it comes right down to it, if an organization has put someone's name on something, it is difficult for the organization to argue that the thing isn't "about" that individual.

The definition is deliberately broad, and in my findings I have tended to interpret it as broadly as possible. Generally speaking, it does not matter who generated the information, or how, or who technically "owns" it, or what the corporate convention may be. If it has been assigned in an individual's name, the chances are that I will accept it as being his or her personal information.

I am inclined to regard information as personal even if there is the smallest potential for it to be about an identifiable individual. A case in point was one in which a broadcaster had attempted – inadvertently, as it turned out – to collect NETBIOS information from the computer of a Web site visitor. Our investigation revealed that, in certain technical circumstances such as the complainant's, NETBIOS information could be used to trace the computer's Internet Protocol address, which in turn could be used to trace Web sites visited by the user or recent passwords to secure accounts. On the basis of the potential for intrusion into the complainant's privacy, I determined that the information at issue was personal information for purposes of the *PIPED Act*.

But even a deliberately broad definition must have limits. In a much-publicized case, I took the view that section 2 was not so broad as to encompass all information associated with an individual. Specifically, I determined that physicians' prescriptions or prescribing patterns did not constitute personal information about

the physicians themselves. An individual prescription, I reasoned, is potentially revealing about a patient, but it is not in any meaningful sense about the prescribing physician as an individual. Rather, it is about the professional process that led to its issuance and should therefore be regarded as a work product – that is, the tangible result of the physician's work activity.

I judged furthermore that extending the definition to include prescriptions and prescribing patterns would not be consistent with the *PIPED Act*'s purpose. Section 3 sets out that purpose in terms of balancing the individual's right of privacy with the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate. I did not think it reasonable to extend the definition to prescriptions, since that would mean extending it also to other work products such as legal opinions or documents written in the course of employment. Nor did I think it reasonable to extend the definition to prescribing patterns, since that would mean extending it also to patterns discoverable in other types of work products and thus would preclude many kinds of legitimate consumer reporting.

Systemic Problems

Privacy code only the beginning

It is the rare organization nowadays that isn't greatly concerned about the privacy rights of individuals – on paper, at least. Most corporate brochures and Web sites proudly proclaim a privacy code, ostensibly in full compliance with corporate obligations under the *PIPED Act*. What our complaint investigations are showing, however, is that some organizations have been less than thorough about putting their codes into practice.

A privacy code is pointless without comprehensive and detailed policies and procedures, and these in turn are pointless unless they are known and consistently observed and applied. The privacy violations that give rise to complaints are often attributable to problems or defects in an organization's information-handling processes or system as a whole. Such problems are themselves often caused by failure on an organization's part to grasp, or turn its attention to, the practical implications of the *PIPED Act*'s principles. Sometimes, too, the problems derive from unquestioned adherence to traditional practices that may no longer be acceptable under the *Act*.

The following are a few of the systemic problems that our investigations have been turning up.

Not designating a privacy officer

Principle 4.1 of Schedule 1 to the *PIPED Act* states that an organization must designate one or more individuals responsible for the organization's compliance with the principles of the *Act*. In more than one case, we have found that the organization had not yet designated such an individual or did not identify any person as the responsible privacy officer.

Not knowing how to handle access requests and complaints

Most organizations seem to understand that an individual has a right to gain access to his or her personal information (Principle 4.9) and to challenge an organization's compliance (Principle 4.10). However, when it comes down to receiving an actual access request or complaint from an individual, some organizations are still uncertain how to go about processing it. At this point, it is especially important to have specific policies and procedures in place and to follow them thoroughly and consistently.

Keeping information too long or not long enough

Retention is another principle to which some organizations need to pay greater heed in the form of specific guidelines and procedures. Under Principle 4.5.2, a minimum and a maximum retention period should be established for personal information. Information that has been used to make a decision about an individual must be kept long enough to allow the individual access to the information. Under Principle 4.5.3, information no longer required to fulfil identified purposes should be destroyed, erased or made anonymous.

What we have been finding in some cases is that organizations are either destroying personal information too soon – that is, before the individual has a chance to gain access to it – or habitually keeping it for long periods of time, far past any need to do so. In one case, we learned of an organization that was in the habit of keeping the information it collected from *unsuccessful* credit card applicants for indefinite periods of time and for no particular reason. We even learned of one organization that never destroyed any of the personal information it collected, just because it didn't know it was allowed to.

Not meeting the time limit

As provided in section 8 of the *PIPED Act*, I have already determined in a number of cases that organizations have in effect refused individuals' access requests by having exceeded the 30-day time limit for response. In most of these cases, however, the failure to meet the time limit was due more to a lack of efficient procedures for processing the requests than to deliberate refusal on the organization's part.

Not limiting collection to what is necessary

Is it appropriate for an organization, such as an Internet company, to insist on having your Social Insurance Number (SIN)? The short answer is no; there are very few private sector organizations that have a legitimate reason for collecting SINs from customers (financial institutions sometimes need to collect them for revenue reporting purposes, for example).

But in one noteworthy complaint last year, collection of SINs was the central issue. In that case, it had been the company's policy for some time to collect SINs as a means of avoiding confusion over similar names among customers. The company had never really considered whether that purpose was a legitimate one, and front-line staff had come to regard the collection as a requirement. In my finding, I determined that the collection was unnecessary and indiscriminate and that it was clearly wrong of the company to require applicants to provide their SINs as a condition of service.

This was not the only case where an organization collected more information than it really needed to fulfil legitimate purposes. Under the *PIPED Act*, organizations must take pains to ensure not only that their purposes for collecting personal information are legitimate and reasonable ones, but also that both the amount and type of information collected are necessary to fulfil those purposes. Reviewing longstanding and long-unquestioned collection policies and practices is the best way for an organization to start complying with Principle 4.7, limiting collection.

Not identifying purpose for which information collected

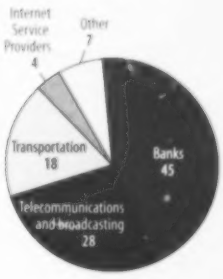
Persons from whom organizations demand information have a right to know why. It is therefore not enough that purposes be legitimate. They must also be identified.

Under Principle 4.2, an organization must identify the purposes for which it collects information. Under Principle 4.2.1, the purposes must be documented. Under Principle 4.2.3, the organization should specify the purposes to the individual at or before the time of collection. And under Principle 4.2.5, it is incumbent on the organization to make sure that employees who do the collecting can explain the purposes to individuals who question the practice.

Several complaints so far have brought to light violations of one or more of these principles. Again, in some cases the cause has been a slowness to understand that standard ways of doing things in the past are not necessarily acceptable now that the *PIPED Act* is with us.

Complaints by Sector

January 1, 2001 to December 31, 2001



Not instituting proper safeguards

In one case last year, I found that an organization's reliance on a credit cardholder's telephone number or year of birth was not adequate to prevent unauthorized access to the individual's personal information. In another case, involving loss of documents, I found that an organization had not taken proper measures to protect personal information during a transfer of files to another building. In yet another, I found that a company was not exercising appropriate operational controls in a workplace to keep employees' pay statements confidential.

In these and other cases involving actual or potential breaches of informational security, the central issue was the adequacy of the safeguards instituted by certain organizations. Principle 4.7 states that personal information must be protected by security safeguards appropriate to the sensitivity of the information. Depending on the nature of the information, safeguards may take many forms, ranging from physical measures such as locked filing cabinets, to organizational measures such as security clearances, to technological measures such as the use of passwords and encryption.

The obligation to protect personal information once it has been collected is obviously one that some organizations need to start taking more seriously.

Not recognizing that employees have privacy rights too

There is considerable evidence that some organizations that are federal works, undertakings or businesses, upon reading that the *PIPED Act* applies to the collection, use and disclosure of personal information, have jumped to the conclusion that it refers only to information about their customers. It appears not to have occurred to such organizations that, in the everyday course of business administration, they also handle a great deal of personal information about the individuals who work for them.

As a result, some organizations have been taken off guard by certain well-founded complaints against them under the *PIPED Act* – complaints filed by their own employees, past or present. In good part, the violations at issue in such complaints originate in an organization's neglect to take its staff into account in developing privacy policies and procedures.

Positive Responses to my Recommendations

Despite the foregoing, I find it encouraging that, once systemic problems have been pointed out to them, organizations by and large have been quick to accept and implement the remedies that I have recommended.

Overall, I am pleased with the progress of the *PIPED Act* so far, and with the efforts that organizations are making to bring themselves into compliance with it.

Definitions of Findings under the *PIPED Act*

Not well-founded: This means that there is no evidence to lead the Privacy Commissioner to conclude that the organization violated the *Personal Information Protection and Electronic Documents (PIPED) Act.*

Well-founded: This means that the investigation revealed that the organization failed to respect a provision of the *PIPED Act.*

Resolved: This means that the organization has taken corrective action to remedy the situation, or that the complainant is satisfied with the results of the inquiries made by the Office of the Privacy Commissioner of Canada.

Discontinued: This category applies to investigations that are terminated before all the allegations have been fully investigated. A case may be discontinued for any number of reasons, for example, when the complainant is no longer interested in pursuing the matter.

Privacy Practices and Reviews

The *Personal Information Protection and Electronics Documents (PIPED) Act* allows me to audit the compliance of private organizations if I have "reasonable grounds to believe" that the organizations are contravening a provision of the *Act* or are not following a recommendation set out in Schedule 1.

The Privacy Practices and Reviews Branch of my Office will conduct compliance reviews and audits under section 18 of the *PIPED Act*, following accepted standard audit objectives and criteria. As I mentioned in my previous *Annual Report to Parliament*, I have not yet initiated any such audit because no matter has been brought to my attention that meets the reasonable grounds test.

In the Courts

Under section 14 of the *Personal Information Protection and Electronic Documents (PIPED) Act*, an individual complainant has a right, following my investigation, to apply to the Federal Court of Canada for a hearing in respect of any matter on which the complaint was made or that is referred to in the Commissioner's report. These matters must be among those in the Schedule clauses and sections of the *Act* listed in section 14. I may also apply to the Court in respect of any complaint I have initiated. From the time the *Act* came into force on January 1, 2001, five applications have been filed in the Federal Court.

Section 15 of the *PIPED Act* allows me to apply to appear in Federal Court. I may, with the consent of the complainant, apply directly to the Court for a hearing in respect of any matter covered by section 14; appear before the Court on behalf of any complainant who has applied under section 14; or, with the leave of the Court, appear as a party to any section 14 hearing.

The following is not an exhaustive list of applications in the courts but a listing of matters of particular interest.

Mathew Englander v. Telus Communications Inc.

This is the first application to be filed in the Federal Court under section 14 of the *PIPED Act*. Mr. Englander argues that Telus uses and discloses customers' names, addresses and telephone numbers in its white pages directories and otherwise, without customers' knowledge and consent, and inappropriately charges customers for choosing to have their telephone number "non-published." He claims that these actions by Telus contravene subsections 5(1) and (3) of the *Act*, as well as several clauses of Schedule 1 of the *Act*.

Status

A hearing date has not been set.

Ronald G. Maheu v. IMS Health Canada and the Privacy Commissioner of Canada

Ronald Maheu applied for a hearing in the Federal Court of Canada, arguing that IMS Health Canada improperly discloses personal information by selling data on physicians' prescribing patterns without their consent.

Status

In his application, Mr. Maheu had asked the Court to review my "decision" in this case. I filed a motion objecting to the manner in which Mr. Maheu had framed his application, arguing that under the *PIPED Act* it is the responsibility of the organization concerned (here, IMS), and not the Privacy Commissioner, to justify why it should not have to modify its practices to comply with the *Act*. On February 12, 2002 the Federal Court ordered Mr. Maheu to file an amended Notice of Application removing allegations and requested orders against my Office, and ordered that his application be directed solely against IMS Health Canada. I was also granted leave under section 15(c) of the *Act* to appear as a party respondent in support of my finding in this proceeding. On May 14, 2002, in response to a motion brought by IMS, the Federal Court ordered Mr. Maheu to post security for costs. Mr. Maheu has successfully appealed this order.

Communications and Public Education

The *PIPED Act* has given me and my Office a greater responsibility, an expanded role and a strengthened legislative mandate to educate Canadians and organizations about issues surrounding personal privacy.

To meet these new responsibilities and in preparation for the communications activities ahead, my Office's communications capabilities were expanded. Since then, we have been proactively involved in a variety of activities to raise public awareness and understanding of issues that could potentially threaten Canadians' privacy, to inform Canadians of their legislated privacy protections and to remind private sector organizations of their responsibilities under the new legislation.

In view of my mandated responsibilities under section 24 of the *Act*, I am gratified by the increased awareness of privacy rights and privacy issues that these activities appear to be generating.

Speaking engagements

Conferences and other special events, in Canada and around the world, have provided me with a unique opportunity to meet Canadians and to raise awareness of privacy issues among diverse audiences and settings – professional and industry associations, non-profit and advocacy groups, universities and public events.

From January 1, 2001 to March 31, 2002, I gave a total of 55 speeches; another 35 were delivered by other senior staff of this Office. At these events, I spoke out about issues such as workplace privacy, genetic privacy, the application of the *PIPED Act* and its implications for businesses, the Government On-Line initiative, my grave concerns regarding video surveillance by public authorities in public places, and the need to balance privacy rights with security objectives following the terrorist attacks in the United States.

At international conferences, I had the opportunity to share my perspective on the Canadian experience with officials and privacy advocates from other countries.

Media relations

The media's appetite for news relating to privacy has continued to increase steadily. Our analysis of news coverage indicates a growing interest in the issues and in awareness of this Office. The number of calls from journalists, which currently averages approximately 100 per month, continues to increase. From January 1, 2001 to March 31, 2002, I granted more than 270 interviews to reporters.

In addition to responding to the demand for more information and comment about personal privacy and Canadians' rights under federal privacy laws, my Office has taken a number of steps to raise awareness of various issues through the media. During this period, we disseminated more than 25 news releases and media advisories, participated in a number of editorial board meetings of daily newspapers across the country, contributed articles and other information to several publications, and provided media relations support for conferences, public meetings and other special events.

Public education materials

In 2001, my Office produced two guides in anticipation of a demand from Canadians and businesses for more information about the *PIPED Act*. Our *Citizens' Guide* tells Canadians about their rights under the new law. The *Business Guide* informs organizations of their responsibilities under the law, so they can learn how to comply with it.

The Office receives requests for these guides on a daily basis and the demand is increasing. Not only are these materials sent to individuals upon request, they are also distributed at conferences and accessed in electronic format by visitors to our Web site. During this period, more than 24,000 of the guides were distributed.

In addition to the *Citizens' Guide* and the *Business Guide*, this Office has produced and distributed other educational and promotional materials, including bookmarks, posters, fact sheets, annual reports and copies of both federal privacy laws.

Plans are currently underway to identify other suitable locations where the guides and the other information could be offered to Canadians.

Advertising

Advertising is another important tool my Office has used to raise public awareness and understanding of privacy issues.

In 2001, we placed advertisements in daily and community newspapers. The ads provided information on the new legislation and its application to federally regulated businesses.

In 2002, we initiated another national advertising campaign. Radio spots were produced in English and French, and were aired on the top stations in every market across the country. These radio ads emphasized Canadians' rights under the new law and my Office's role in helping to protect those rights.

Both advertising campaigns reached millions of Canadians and resulted in nearly doubling the number of inquiries to this Office.

Public inquiries

The Communications and Policy Branch also responds to thousands of inquiries from the general public who contact my Office for advice and assistance on all sorts of privacy-related matters.

Web site

In the spirit of openness and transparency, every effort is made to ensure that new and useful information is posted on my Office's Web site on an ongoing basis and in a timely manner. New elements such as speeches, news releases, fact sheets, selected reports and case summaries are always being added to keep the site current and interesting.

Over the past year, because organizations wanted a better understanding of how the *PIPED Act* was being applied, a new section entitled "Commissioner's Findings" was added to the site. Here, summaries of my findings are posted in an effort to provide guidance to businesses and the legal community.

In 2001, the Web site was redesigned and the number of visits to the Web site has increased steadily, with a surge that resulted in almost double the visitors after October 2001. Over the period, the site averaged approximately 16,000 hits per month.

Communications Activities

January 1, 2001 to March 31, 2002

Activity		Number
Speeches delivered by Privacy Commissioner		55
Speeches delivered by senior staff		35
News releases		25
Media interviews		270
Distribution of materials		**34,036**
Business Guides	14,170	
Citizens' Guides	10,666	
Other (Annual Reports, bookmarks, fact sheets, *Acts*, etc.)	9,200	
Average number of visits to Web site per month		16,079

Inquiries by type under *Privacy Act*

April 1, 2001 to March 31, 2002

Subject	Number
Adoption/genealogy	35
Access to personal information *	504
Census	297
Collection, use and disclosure *	224
Consent issues *	25
Corrections *	18
Criminal records, pardons	203
E-311 Travel Declaration Form **	26
Firearms	76
Law enforcement *	60
Medical records **	98
No jurisdiction (federal)	983
Office of the Privacy Commissioner of Canada *	111
Personal health information *	49
Privacy Act, interpretation and process	6,988
Publication requests	189
Redirect – external	3,240
Social Insurance Numbers	410
Video surveillance *	50
Workplace surveillance *	13
Calls from Members of Parliament	31
Other	642
Total	**14,272**

* These categories were compiled from January to March 2002 only.
** These categories were compiled from April to December 2001 only.

Inquiries by type under the *PIPED Act*

January 1, 2001 to December 31, 2001

Subject	Number
Criminal records	31
Drug testing	3
Encryption	7
Financial institutions	1,609
Identity theft	38
Information request	2,744
Interception/monitoring	154
PIPED Act, interpretation and process	2,151
Jurisdiction	2,103
Marketing	462
Medical records	144
Publication requests	679
Social Insurance Number	1,902
Telecommunications	827
Transportation	152
Calls from Members of Parliament	7
Other	388
Total	**13,401**

Part Three Corporate Services

In order to manage the implementation of the *PIPED Act*, and because of an increased mandate under the *Act*, my Office has experienced an increase in resources, both human and financial.

On April 1, 2001, my Office's budget was increased to $11.1 million from $8.7 million the previous year, and will be maintained for the next fiscal year to support the following:

- An increase in communications activities, inquiries and complaints;
- An increase in the number of investigators, auditors and Privacy Impact Assessment officers to handle issues in relation to both federal privacy laws;
- An extension of our hours of operation – now from 9 a.m. to 5 p.m. in all time zones across Canada;
- The establishment of a solid management framework which incorporates both the investigative and audit functions of the Office; and
- The establishment on April 1, 2002 of a dedicated corporate services branch for this Office, for information technology, human resources, finance and administration purposes (previously, corporate services were shared with the Office of the Information Commissioner).

In preparation for the full implementation of the *PIPED Act* on January 1, 2004, a financial framework for funding will be presented to the Treasury Board Secretariat to substantiate future expenditures.

Resources

April 1, 2001 to March 31, 2002

	FTEs	Expenditure Totals	Percentage of Total
Privacy	93	$ 9,435,901	82%
Corporate Services	15	$ 2,021,867	18%
Total	**108**	**$11,457,768**	**100%**

Note: FTE stands for "full-time equivalent" or full-time staff as of March 2002.

Detailed Expenditures

April 1, 2001 to March 31, 2002

	Privacy	Corporate Services	Total
Salaries	$5,101,779	$1,078,633	$ 6,180,412
Employee Benefits Program	1,172,850	167,150	1,340,000
Transportation and Communication	446,109	132,985	579,094
Information	1,566,375	7,502	1,573,877
Professional Services	656,962	223,749	880,711
Rentals	11,412	20,923	32,335
Repairs and Maintenance	50,453	19,920	70,373
Materials and Supplies	99,053	40,494	139,547
Acquisition of Machinery and Equipment	298,673	330,147	628,820
Other Subsidies and Payments	32,235	364	32,599
Total	**$9,435,901**	**$2,021,867**	**$11,457,768**

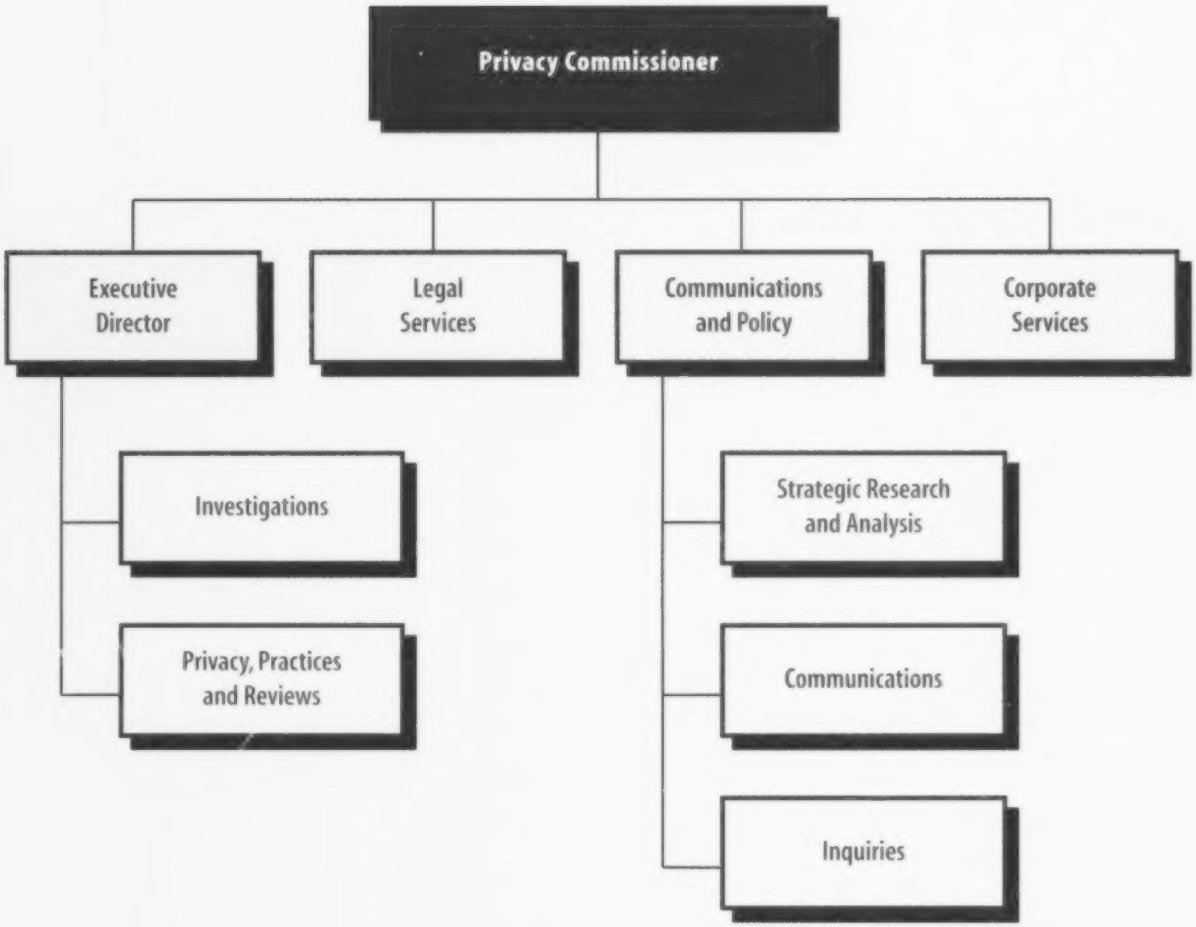
Notes:

[1] Total expenditure figures are consistent with public accounts.

[2] Expenditures for Corporate Services were allocated on a 50/50 basis and shared between the Offices of the Privacy Commissioner of Canada and the Information Commissioner of Canada.

[3] Effective April 1, 2002, Corporate Services is part of this Office and services are no longer shared with the Office of the Information Commissioner of Canada.

Corporate Structure

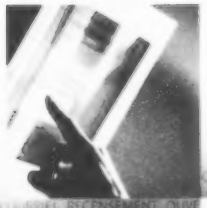


- Effective April 1, 2002, Corporate Services is part of this Office and resources are no longer shared with the Office of the Information Commissioner of Canada.

Commissaire à la protection de la vie privée du Canada

The Privacy Commissioner of Canada

Rapport annuel au Parlement 2001-2002



Commissaire à la protection
de la vie privée du Canada

The Privacy Commissioner
of Canada

Rapport annuel
au Parlement
2001-2002

Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-8210, 1-800-282-1376
Téléc. (613) 947-6850
ATS (613) 992-9190

N° de cat. IP30-1/2002
ISBN 0-662-66668-2

Cette publication est également disponible sur notre site Web à **www.privcom.gc.ca**

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél.: (613) 995-8210
Téléc.: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Janvier 2003

L'honorable Daniel Hays
Président
Sénat du Canada

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1er avril 2001 au 31 mars 2002 conformément à la *Loi sur la protection des renseignements personnels* et du 1er au 31 décembre 2001 conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

À l'origine, la parution de ce rapport était prévue pour le printemps dernier. Néanmoins, l'année 2002 fut tumultueuse au point de vue de la protection de la vie privée, et j'étais plutôt hésitant à le présenter au Parlement étant donné que des principaux dossiers, particulièrement les dossiers liés à l'équilibre essentiel entre la protection de la vie privée et la sécurité soulevée à la suite des événements du 11 septembre, n'ont pas été résolus. Conformément à mon mandat en tant qu'ombudsman des droits de la protection de la vie privée des Canadiens et des Canadiennes, j'ai continué à chercher des solutions à ces problèmes avec l'aide des ministres et des hauts fonctionnaires. Malgré la prolongation répétée de mes échéances, je n'ai, jusqu'à maintenant, connu aucun succès. Je ne peux visiblement pas demander au Parlement d'attendre indéfiniment et je dois présenter mon rapport malgré la situation non concluante et insatisfaisante.

Je rédigerai un rapport sur mon expérience acquise au cours de cette deuxième année de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels et les documents électroniques* dans mon prochain rapport annuel.

Le Commissaire à la protection
de la vie privée du Canada,

George Radwanski

Office of the Privacy Commissioner of Canada

112 Kent Street
Ottawa, Ontario
K1A 1H3
Tel.: (613) 995-8210
Fax: (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Commissariat à la protection de la vie privée du Canada

112, rue Kent
Ottawa (Ontario)
K1A 1H3
Tél. : (613) 995-8210
Télec. : (613) 947-6850
1-800-282-1376
www.privcom.gc.ca

Janvier 2003

L'honorable Peter Milliken
Président
Chambre des communes

Monsieur,

J'ai l'honneur de remettre au Parlement mon rapport annuel pour les périodes du 1er avril 2001 au 31 mars 2002 conformément à la *Loi sur la protection des renseignements personnels* et du 1er au 31 décembre 2001 conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*.

À l'origine, la parution de ce rapport était prévue pour le printemps dernier. Néanmoins, l'année 2002 fut tumultueuse au point de vue de la protection de la vie privée, et j'étais plutôt hésitant à le présenter au Parlement étant donné que des principaux dossiers, particulièrement les dossiers liés à l'équilibre essentiel entre la protection de la vie privée et la sécurité soulevée à la suite des événements du 11 septembre, n'ont pas été résolus. Conformément à mon mandat en tant qu'ombudsman des droits de la protection de la vie privée des Canadiens et des Canadiennes, j'ai continué à chercher des solutions à ces problèmes avec l'aide des ministres et des hauts fonctionnaires. Malgré la prolongation répétée de mes échéances, je n'ai, jusqu'à maintenant, connu aucun succès. Je ne peux visiblement pas demander au Parlement d'attendre indéfiniment et je dois présenter mon rapport malgré la situation non concluante et insatisfaisante.

Je rédigerai un rapport sur mon expérience acquise au cours de cette deuxième année de l'entrée en vigueur de la *Loi sur la protection des renseignements personnels et les documents électroniques* dans mon prochain rapport annuel.

Le Commissaire à la protection
de la vie privée du Canada,

George Radwanski

Table des Matières

Compte rendu du Commissaire 1

Première partie – Rapport concernant la *Loi sur la protection des renseignements personnels* 25

Introduction 25

Enquêtes 26

Plaintes en vertu de la *Loi sur la protection des renseignements personnels*. 27

Définition de conclusions aux termes de la *Loi sur la protection des renseignements personnels* 28

Sommaire de cas choisis en vertu de la *Loi sur la protection des renseignements personnels* . . 29

Les ministères sont responsables des renseignements recueillis en vertu d'un marché. 29

La GRC exige des frais pour les rapports d'analyse de la circulation. 31

Le MDN conserve et utilise indûment des renseignements sur des délinquants réhabilités. . 32

La demande de renseignements sur l'impôt par la SCHL est inappropriée 33

Surveillance indue des comptes de courrier électronique d'employés 35

Un homme se voit refuser l'accès à ses renseignements personnels à la suite d'une enquête sur les crimes de guerre 37

La communication de renseignements durant un appel doit être limitée 38

La Société canadienne des postes modifie sa position concernant le recours au consentement négatif pour vendre des adresses aux expéditeurs de courrier grand public 41

Incidents visés par la *Loi sur la protection des renseignements personnels*. 43

Communication inappropriée du NAS sur les formulaires de prestations fiscales canadiennes pour enfants 43

Des documents du registre des armes à feu trouvés dans un conteneur 44

DRHC et l'ADRC partagent des données sur l'admissibilité au Supplément de revenu garanti 45

Communications dans l'intérêt public 47

Examens et pratiques en matière de vie privée 55
Introduction 55
Le point sur le Programme canadien des armes à feu 57
Mise à jour du Protocole de gestion DRHC pour le Comité d'examen des banques de données 58
Devant les tribunaux 61
Introduction 61
Formulaires de déclaration du voyageur (E-311) 61
Commissaire à l'information du Canada c. Commissaire de la GRC et Commissaire à la protection de la vie privée 62
Clayton Charles Ruby c. Solliciteur général 63
Robert Lavigne c. Commissariat aux langues officielles 64
Commissaire à l'information de Canada c. Ministre de Citoyenneté et Immigration Canada et Philip W. Pirie 65
Mertie Anne Beatty et al. c. Statisticien en chef et al. 66
Deuxième partie – Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques* 67
Introduction 67
La définition de renseignements personnels : de portée vaste mais non infinie 67
Problèmes systémiques 69
Le code type sur la protection des renseignements personnels, ce n'est qu'un début . . . 69
Défaut de désigner un agent à la protection de la vie privée 70
Méconnaissance du traitement des demandes d'accès et des plaintes 70
Conservation trop longue ou trop courte des renseignements 70
Non-respect des échéances 71
Collecte excessive de renseignements 71
Défaut d'identifier des fins pour lesquelles les renseignements sont recueillis 71
Absence de mesures de sécurité convenables 72
Méconnaissance du fait que les employés ont également des droits à la vie privée 72

Réponses positives à mes recommandations 73

Définitions aux termes de la *LPRPDÉ*. 73

Examens et pratiques en matière de vie privée 74

Devant les tribunaux 74

Mathew Englander c. Telus Communications Inc. 75

Ronald G. Maheu c. IMS Health Canada et Commissaire à la protection de la vie privée du Canada 75

Communications et sensibilisation du public 76

Allocutions 76

Relations médiatiques 77

Documents de sensibilisation du public 77

Publicité 78

Demandes de renseignements du public 78

Site Web 78

Troisième partie – Services de gestion 83

Ressources 84

Dépenses détaillées 85

Structure organisationnelle 86

Compte rendu du Commissaire

Il est de mon devoir, dans le présent rapport annuel, de lancer un avertissement formel et pressant à chaque député et à chaque sénateur et, de fait, à chaque Canadien et Canadienne :

Le droit fondamental de la personne à la protection de la vie privée au Canada est, plus que jamais, gravement menacé. À moins que les parlementaires et l'opinion publique ne se mobilisent rapidement pour dissuader le gouvernement du Canada de poursuivre dans la même voie, nous risquons de perdre définitivement non seulement des droits à la vie privée que nous considérons comme acquis, mais aussi des aspects importants de la liberté que nous connaissons aujourd'hui.

Nous courons ce risque à cause des conséquences, tant individuelles que cumulatives, d'une série de mesures que le gouvernement a prises ou qu'il se prépare à prendre. Ces mesures ont pour toile de fond les événements du 11 septembre et visent en principe à combattre le terrorisme. Toutefois, les aspects qui menacent le plus la vie privée n'ont aucun lien avec la lutte contre le terrorisme, ou n'offrent aucune promesse convaincante d'améliorer efficacement la sécurité.

Finalement, le gouvernement utilise les événements du 11 septembre comme excuse pour justifier de nouvelles collectes et utilisations de renseignements personnels sur nous tous, les Canadiens et Canadiennes. Ces mesures ne peuvent justifier les besoins de la lutte contre le terrorisme et, par le fait même, n'ont pas leur place dans une société libre et démocratique.

Au moment où ce rapport devait aller sous presse, le 17 janvier, le gouvernement n'a démontré aucune volonté à modifier les initiatives en réponse aux préoccupations relatives à la protection des renseignements personnels. Je ne suis pas en mesure de savoir si le gouvernement, sachant que la sortie de ce rapport serait imminent, aurait apporté des changements d'ici au dépôt du rapport.

George Radwanski
Commissaire à la protection de la vie privée du Canada

J'aimerais souligner, d'entrée de jeu, que je n'ai jamais, en aucune circonstance, soulevé d'objections fondées sur la protection de la vie privée relativement à la moindre mesure de protection contre le terrorisme. De fait, j'ai affirmé à maintes reprises, depuis le 11 septembre, que je ne chercherais jamais, en ma qualité de Commissaire à la protection de la vie privée, à m'opposer à une mesure quelconque qui pourrait légitimement s'avérer nécessaire pour accroître la protection contre le terrorisme, même si elle devait empiéter sur le droit à la vie privée ou le limiter.

Je me suis opposé uniquement à l'élargissement des soi-disant mesures anti-terroristes pour servir d'autres buts qui n'ont absolument rien à voir avec la lutte contre le terrorisme, ou à des atteintes à la vie privée dont la pertinence ou la nécessité n'ont nullement pu être démontrées dans le cadre de la lutte contre le terrorisme. Et pourtant, le gouvernement continue de faire la sourde oreille.

Je parle plus précisément de la nouvelle base de données sur les voyageurs, du style *Big Brother*, de l'Agence des douanes et du revenu du Canada ; des dispositions de l'article 4.82 du projet de loi C-17 ; des pouvoirs sérieusement accrus de l'État relativement à la surveillance de nos communications, tels qu'ils sont décrits dans le document de consultation « Accès légal » ; de la carte d'identité nationale comportant des identificateurs biométriques que propose le ministre de la Citoyenneté et de l'Immigration, Denis Coderre ; et de l'appui du gouvernement à une mesure qui établira un précédent en matière de surveillance vidéo des voies publiques par la GRC.

Ces mesures suscitent de profondes inquiétudes en raison des atteintes directes à la vie privée qu'elles comportent. Elles sont d'autant plus troublantes parce qu'elles transgressent des seuils et ouvrent des portes. Chacune de ces mesures établit un nouveau principe terriblement dangereux d'atteinte acceptable à la vie privée.

La base de données de l'ADRC fait entrer en scène la création de dossiers de renseignements personnels sur tous les citoyens respectueux de la loi pour un large éventail de sujets d'enquête. L'article 4.82 du projet de loi C-17 exige, pour la première fois, l'auto-identification obligatoire *de facto* à la police à des fins d'application générale de la loi. Le document « Accès légal » prône la surveillance généralisée de nos activités de communication et de nos habitudes de lecture.

Une carte d'identité nationale nous ferait perdre le droit à l'anonymat dans notre quotidien. La surveillance vidéo par la GRC n'est ni plus ni moins qu'une observation systématique, par la police, des citoyens vaquant à leurs occupations légitimes sur les voies publiques.

Il ne s'agit pas ici d'inquiétudes abstraites ou théoriques. Si nous permettons l'entrée en vigueur de ces mesures et acceptons les principes d'atteinte à la vie privée qu'elles représentent, il se pourrait bien que, d'ici peu, nos vies au Canada ressemblent fort à ce qui suit :

- Tous nos séjours à l'extérieur du Canada seront systématiquement enregistrés, observés et analysés dans le but de repérer des signes de ce que le gouvernement pourrait trouver douteux ou indésirables. Des dossiers « Orwelliens » de renseignements personnels sur chaque Canadienne et Canadien respectueux de la loi – contenant à l'origine des renseignements sur les voyages, mais auxquels se seront éventuellement ajoutés Dieu seul sait quoi – seront tenus par le gouvernement fédéral et accessibles à pratiquement tous les ministères et organismes fédéraux, juste au cas où il pourrait être pratique de les utiliser contre nous.
- Pour chaque voyage effectué à l'intérieur du Canada, nous devrons nous identifier à la police pour que leurs ordinateurs puissent vérifier si nous sommes recherchés pour quelque raison que ce soit, ou si l'État s'intéresse à nous d'une manière ou d'une autre.
- Les services de police et de sécurité pourront avoir accès à des enregistrements de chaque message électronique que nous avons envoyé et de chaque appel que nous avons fait au moyen d'un téléphone cellulaire. Des renseignements sur ce que nous lisons dans Internet, sur chaque site et chaque page Web que nous consultons, seront tout aussi facilement à la disposition des autorités gouvernementales.
- Le gouvernement prendra les empreintes digitales et rétiniennes de tout le monde. Ces renseignements biométriques figureront sur des cartes d'identité nationales obligatoires qui permettront à la police de nous arrêter sur la voie publique et de nous obliger à nous identifier sur demande.
- Nos allées et venues sur les voies publiques seront observées sans relâche par des caméras policières de surveillance vidéo toujours plus nombreuses. Ces caméras finiront éventuellement par être reliées à des appareils de reconnaissance biométrique des visages qui compareront nos images sur l'écran à des photos en dossier – provenant de permis de conduire, de passeports ou de cartes d'identité – et permettront à la police de connaître notre nom et notre adresse, alors que nous vaquons à nos activités légitimes sur les voies publiques.

SI ON LAISSE LE GOUVERNEMENT POURSUIVRE SES INITIATIVES ACTUELLES, IL Y A UN RISQUE TRÈS RÉEL QUE NOTRE DROIT À LA VIE PRIVÉE, TEL QUE NOUS LE CONNAISSONS, NE SOIT BIENTÔT PLUS QU'UN SOUVENIR LOINTAIN ET IRRÉCUPÉRABLE.

Je sais bien que ces scénarios peuvent paraître des exagérations alarmistes aux yeux de la plupart des gens. Certes, la société que je décris ne ressemble en rien au Canada que nous connaissons. Mais quiconque serait enclin à balayer les risques du revers de la main devrait prendre le temps de réfléchir à la situation et de se rendre compte que les mesures d'incursion dans la vie privée déjà mises en place ou en voie de l'être auraient été inconcevables dans notre pays il y a à peine un an.

Je ne prédis pas que tous ces scénarios vont nécessairement se réaliser. Mais j'affirme énergiquement que, chaque fois qu'un principe est accepté et qu'un précédent est établi, d'autres incursions dans la vie privée ne sont qu'une question d'échelonnement, et sont donc pratiquement inévitables.

C'est au tout début qu'il faut bloquer les atteintes non justifiées à un droit fondamental de la personne tel le droit à la vie privée, chaque fois que l'État tente de s'immiscer là où il n'a pas sa place. Autrement, le terrain aura été concédé et la bataille perdue.

C'est pourquoi si on laisse le gouvernement poursuivre ses initiatives actuelles, il y a un risque très réel que notre droit à la vie privée, tel que nous le connaissons, ne soit bientôt plus qu'un souvenir lointain et irrécupérable.

La situation est d'autant plus inquiétante que le gouvernement fait tout cela à découvert, au mépris flagrant et répété des préoccupations qu'il est de mon devoir d'exprimer en tant que haut fonctionnaire du Parlement chargé de superviser et de défendre les droits à la vie privée de tous les Canadiens et Canadiennes.

Ce mépris met en péril les droits à la vie privée des Canadiens et Canadiennes non seulement directement, par l'application des mesures envahissantes en question, mais aussi indirectement en sapant l'édifice entier de la protection de la vie privée qui existe dans notre pays depuis près de vingt ans.

Malheureusement, ce gouvernement a perdu tout repère moral en ce qui concerne le droit fondamental de la personne à la vie privée.

Il semble convaincu que le droit à la vie privée doit être sacrifié petit à petit, de jour en jour, au profit d'objectifs plus importants : rassurer un public effrayé par l'horreur du 11 septembre ; apaiser un gouvernement américain insistant ; répondre aux vœux de la police, des services de sécurité et d'autres entités fédérales qui ont vu en l'après-11 septembre une occasion d'étendre leurs pouvoirs.

De plus, le gouvernement est devenu disposé, très mal à propos, à faire fi de toute critique de ses attaques sur les droits à la vie privée, apparemment convaincu que de telles critiques ne sont que la rançon de l'action.

Le mépris du gouvernement pour des droits à la vie privée d'une importance cruciale ne s'affiche plus seulement que dans des cas isolés, il devient systématique. Le droit fondamental de chaque Canadien et Canadienne est donc profondément compromis.

Ces critiques n'émanent pas que de moi dans l'exercice des fonctions que m'a confié le Parlement de la surveillance et de la défense des droits à la vie privée des Canadiens et Canadiennes, mais aussi de bien d'autres sources qui ont fait publiquement écho à mes préoccupations. Parmi elles, notons sept commissaires provinciaux et territoriaux à l'information et à la protection de la vie privée des quatre coins du Canada, l'Association canadienne des libertés civiles, la *B.C. Civil Liberties Association*, la *B.C. Freedom of Information and Privacy Association*, la Ligue des droits et libertés, l'*Electronic Frontier Canada*, le *Commonwealth Centre for e-Governance*, le *Public Interest Advocacy Centre* et l'Association des droits et libertés du Manitoba.

En près de 20 ans d'histoire de la protection de la vie privée, depuis que le poste de Commissaire à la protection de la vie privée a été créé par la *Loi sur la protection des renseignements personnels* en 1983, une convention a été établie : lorsque le Commissaire à la protection de la vie privée signale qu'une pratique ou qu'une mesure est incompatible avec les droits à la vie privée, le gouvernement en tient compte.

C'est de cette façon que le système est censé de fonctionner. Je suis un ombudsman, mandaté par le Parlement, qui m'acquitte généralement de mon rôle à l'égard du gouvernement fédéral par la persuasion et la discussion coopérative loin du regard du public. Comme mes prédécesseurs, c'est ainsi que je m'efforce de travailler depuis ma nomination. J'ai recommandé à des ministres et à de hauts fonctionnaires du gouvernement des solutions particulières qui leur permettaient d'atteindre leurs objectifs politiques légitimes de façon plus respectueuse du droit à la vie privée. Cette méthode a permis d'arriver à plusieurs résultats positifs qui, en raison de la nature même du processus, ne sont pas connus du public.

Mais, dans son approche de l'après-11 septembre, le gouvernement tourne de plus en plus de dos à la nature coopérative du système fédéral de protection de la vie privée en faisant tout simplement la sourde oreille à mes conseils. Dans chaque cas où j'ai dû critiquer publiquement le gouvernement pour n'avoir pas su respecter les droits à la vie privée des Canadiens et Canadiennes, ce n'est qu'après avoir fait tout en mon pouvoir pour convaincre le ministre concerné par des arguments minutieusement raisonnés, et après avoir constaté que le gouvernement ne tenait aucun compte de l'expression de mes préoccupations ou les balayait du revers de la main.

Maintenant, je dois informer le Parlement que, de toute évidence, le mépris du gouvernement pour des droits à la vie privée d'une importance cruciale ne s'affiche plus seulement que dans des cas isolés, il devient

systématique. Le droit fondamental de chaque Canadien et Canadienne est donc profondément compromis. Cette tendance doit être renversée sans délai.

Si le gouvernement peut, en toute impunité et sans susciter de réaction vigoureuse de la part du Parlement, rejeter du revers de la main les mises en garde du Commissaire à la protection de la vie privée et faire ce que bon lui semble, alors la protection de la vie privée dans notre pays sera progressivement dépouillée de son sens et des incursions de plus en plus graves dans la vie privée deviendront inévitables.

Dans les mois qui ont suivi la tragédie du 11 septembre, j'avais l'heureuse impression que, relativement aux droits à la vie privée, le gouvernement proposait dans l'ensemble une réponse équilibrée et réfléchie. Mais les vannes semblent à présent avoir cédé.

Maintenant, le « 11 septembre » est invoqué comme une sorte d'incantation magique, pour étouffer les débats, pour dénigrer l'analyse critique et pour nous persuader que nous vivons dans un monde soudainement nouveau dans lequel les vieilles règles n'ont plus cours.

Si le Parlement et le grand public ont réagi si lentement, c'est probablement parce que, pour la plupart des gens, la plupart du temps, le droit à la vie privée est un concept assez abstrait. Comme dans le cas de notre santé, nous avons l'habitude de n'y penser que lorsqu'elle nous fait défaut – et nous découvrons alors que nos vies ont été changées de façon très déplaisantes, peut-être même de manière irréversible.

Cependant, bien que nous ayons tendance à le tenir pour acquis, le droit à la vie privée – le droit de contrôler l'accès à nous-mêmes et aux renseignements personnels nous concernant – est essentiel à nos vies. Il s'agit d'un droit fondamental de la personne, précisément parce qu'il découle d'un besoin inné de l'être humain, une condition fondamentale de notre liberté, de notre dignité et de notre sentiment de bien-être.

Si quelqu'un s'immisçait dans notre vie privée, que ce soit en pénétrant dans notre foyer, en fouillant dans les effets personnels de notre bureau, en lisant par-dessus notre épaule dans l'autobus ou dans l'avion, ou en écoutant nos conversations, nous nous sentirions mal à l'aise, voire violés.

Imaginez, donc, comment nous nous sentirions s'il devenait coutumier que les bureaucrates, les agents de police et d'autres représentants de l'État se mêlent de tous les détails de nos vies : où et quand nous voyageons, et avec qui ; qui sont les amis et connaissances avec lesquels nous avons des conversations téléphoniques ou échangeons des messages électroniques ; ce que nous lisons et les sujets sur lesquels nous effectuons des recherches ; où nous aimons aller et ce que nous aimons faire.

LE DROIT DE NE PAS SE RÉVÉLER MALGRÉ SOI – EN FAIT, LE DROIT D'ÊTRE ANONYME SAUF LORSQUE NOUS CHOISISSONS DE NOUS IDENTIFIER – EST LE NOYAU DE LA DIGNITÉ, DE L'AUTONOMIE ET DE LA LIBERTÉ HUMAINES.

Nous nous faisons souvent dire : « Si vous n'avez rien à cacher, vous n'avez rien à craindre. »

Si nous acceptons ce raisonnement, bien sûr, il nous importera peu que la police puisse pénétrer dans nos maisons à n'importe quel moment juste pour y jeter un coup d'œil, que toutes nos conversations téléphoniques soient surveillées, que tout notre courrier soit lu, que toutes les protections que nous avons élaborées au fil des siècles soient balayées. Entre ce résultat et les mesures portant atteinte à la vie privée déjà mises en œuvre ou envisagées, il n'y a qu'un pas.

La vérité, c'est que nous avons *tous* quelque chose à cacher, non pas des actes criminels ou même honteux, mais tout simplement parce qu'il s'agit de notre vie privée. Nous mesurons soigneusement ce que nous révélons de nous-mêmes à autrui. La plupart d'entre nous ne sommes disposés à nous laisser connaître que bien peu par un étranger, un peu plus par une connaissance, et le mieux par un ami intime, ou un ou une amie de cœur. Le droit de ne pas se révéler malgré soi – en fait, le droit d'être anonyme sauf lorsque nous choisissons de nous identifier – est le noyau de la dignité, de l'autonomie et de la liberté humaines.

Si nous permettons à l'État d'abattre les cloisons normales de la confidentialité qui protègent les détails de nos vies, nous nous résignons psychologiquement à vivre au vu et au su de tous. Même si nous n'en subissions aucun préjudice particulier, cela changerait profondément ce que nous ressentons. Quiconque a vécu dans une société totalitaire peut en témoigner : le plus opprimant, souvent, est précisément l'absence de vie privée.

Mais il y aura aussi des dangers plus tangibles et particuliers.

Plus le gouvernement accumulera de renseignements sur notre compte, plus il y aura de ces renseignements qui seront erronés. C'est une réalité inéluctable.

Il y a plusieurs années, après l'annonce au grand public par mon prédécesseur de l'existence du « fichier longitudinal sur la main-d'œuvre » de Développement des ressources humaines Canada, de nombreuses personnes ont exigé de voir les renseignements les concernant. Elles ont été ébahies par le nombre d'erreurs constatées. Le fichier n'était qu'une base de données de recherche, dont les inexactitudes n'auraient probablement pas eu beaucoup de conséquences même s'il n'avait pas été démantelé.

Mais si notre vie privée est enfreinte de plus en plus systématiquement par l'État à des fins d'évaluation de notre comportement et de jugements sur notre compte, les renseignements erronés et les fausses interprétations risquent fort d'avoir des conséquences.

Si les renseignements personnels qui proviennent en fait d'une autre personne nous sont faussement associés, si des faits erronés nous font paraître responsables d'actes que nous n'avons pas commis, si un comportement parfaitement innocent est mal interprété et jugé suspect parce que les autorités ne connaissent pas nos raisons ou notre situation, nous risquons d'avoir des ennuis avec une société où tous sont suspects. Avant que nous n'ayons pu laver notre nom et établir notre innocence, nous pourrions avoir subi un préjudice financier ou social irréparable.

Pis encore, nous pourrions ne jamais savoir de quelles hypothèses nuisibles nous avons fait l'objet ni quels jugements négatifs ont été portés sur nous dans les dossiers de l'État. En vertu d'exemptions au droit général d'accès conformément à la *Loi sur la protection des renseignements personnels*, les Canadiens et Canadiennes n'ont pas le droit de voir les renseignements personnels que conserve le gouvernement sur eux si ces données se rapportent à la sécurité nationale ou à une enquête en cours.

Des décisions préjudiciables pourraient se fonder sur des faits erronés, des renseignements incomplets ou hors contexte, ou des hypothèses incorrectes, sans que nous ayons jamais la possibilité de les découvrir, encore moins d'y apporter des corrections.

Avec le temps, cette seule possibilité nous obligera à y penser deux fois avant de faire quelque chose, d'aller quelque part, de nouer des relations, parce que nous aurons appris à nous préoccuper des apparences de nos actions aux yeux omniprésents de l'État.

- Vous avez visité brièvement la Thaïlande au cours d'un voyage d'affaires, et avez tellement aimé le pays que vous pensez y retourner en vacances. Mais des voyages répétés en Thaïlande pourraient-ils vous faire remarquer par les analystes du gouvernement comme un pédophile possible s'y rendant pour le commerce du sexe avec les enfants? Pourriez-vous être détenu et subir un interrogatoire chaque fois que vous faites un voyage? Pourrait-on vous refuser une autorisation de sécurité ou l'entrée aux États-Unis?

- Pour vous détendre, vous naviguez dans Internet et, par curiosité pure et simple, vous vous demandez quel genre de propagande en faveur d'Al-Qaïda pourrait être actuellement diffusée par différents extrémistes. Mais la visite de tels sites Web pourrait-elle vous faire repérer comme terroriste potentiel vous-même, et amener des agents du SCRS ou de la GRC à votre porte?

SI NOUS DEVONS VIVRE NOS VIES EN PESANT CHAQUE ACTION, CHAQUE COMMUNICATION, CHAQUE CONTACT HUMAIN, EN NOUS DEMANDANT CE QUE LES AGENTS DE L'ÉTAT POURRAIENT Y DÉCOUVRIR, Y ANALYSER, EN JUGER, PEUT-ÊTRE MAL INTERPRÉTER ET, D'UNE FAÇON OU D'UNE AUTRE, UTILISER À NOTRE DÉTRIMENT, NOUS NE SOMMES PAS VRAIMENT LIBRES.

- Un étranger vous arrête dans la rue et vous demande des indications. Mais si, à ce moment-là, les voies publiques sont toutes équipées de caméras de surveillance prolifiques reliées à une technologie biométrique de reconnaissance des visages, que se passera-t-il si le système identifie immédiatement l'étranger comme étant un présumé terroriste ou un terroriste connu? Si l'agent de police réussit à avoir votre nom et votre adresse en comparant l'image à l'écran avec la photographie de votre permis de conduire ou de votre passeport, votre dossier sera-t-il classé dans des fichiers de sécurité? Serez-vous identifié comme étant une personne suspecte à la rencontre d'un présumé terroriste dans la rue? Seriez-vous mieux de poursuivre votre chemin lorsqu'une personne essaie de vous adresser la parole?

En fin de compte, si nous devons vivre nos vies en pesant chaque action, chaque communication, chaque contact humain, en nous demandant ce que les agents de l'État pourraient y découvrir, y analyser, en juger, peut-être mal interpréter et, d'une façon ou d'une autre, utiliser à notre détriment, nous ne sommes pas vraiment libres.

Ce genre de vie est caractéristique des pays totalitaires, et non d'une société libre et ouverte comme le Canada. Mais nous nous dirigeons inexorablement vers cette direction si le gouvernement va de l'avant avec ses initiatives actuelles.

Permettez-moi de parler brièvement d'aspects particuliers de ces initiatives inadmissible avant de traiter de certaines considérations plus générales qui, selon moi, devraient nous guider dans la conjoncture de l'après-11 septembre.

La base de données *Big Brother* de l'ADRC

À la fin de 2001, en vertu de modifications apportées à la *Loi sur les douanes*, les agents des douanes de l'ADRC ont reçu l'accès à l'information préalable sur les voyageurs (IPV) et au dossier passager (DP) beaucoup plus détaillé relativement à tous les voyageurs arrivant de l'étranger par avion au Canada. La fin convenue de cette mesure était de recenser les personnes pour lesquelles il convenait de poser des questions plus pointues ou pour lesquelles il convenait de s'intéresser de plus près à leur arrivée.

Lorsque ce projet de loi a été présenté au Parlement, j'ai demandé et obtenu un engagement formel, par écrit, de l'ADRC déclarant que, à l'exception des rares cas où les renseignements relatifs à l'IPV/DP justifieraient qu'une personne soit retenue pour une deuxième série de vérifications, tous les renseignements seraient supprimés dans les 24 heures subséquentes. Fort de cet engagement sans équivoque selon lequel les renseignements ne seraient pas conservés à grande échelle, je n'ai pas exprimé d'objections fondées sur la protection de la vie

privée contre la remise aux Douanes de ces renseignements sur les voyageurs et je n'ai pas jugé nécessaire de témoigner devant les comités de la Chambre des communes et du Sénat faisant l'étude des modifications proposées.

L'été dernier, l'ADRC m'a appris que, contrairement à l'engagement qu'elle avait pris, elle avait décidé de conserver pendant six ans, dans une vaste base de données, tous les renseignements relatifs à l'IPV/DP sur les voyageurs canadiens.

Tous ces renseignements personnels – plus de 30 éléments de données, dont toutes les destinations de nos voyages, les noms des personnes avec qui nous voyageons, le mode de paiement de nos billets (y compris, parfois, les numéros de cartes de crédit), les numéros de contact que nous fournissons, et même nos préférences alimentaires ou exigences liées à la santé que nous indiquons à la compagnie aérienne – seront accessibles pour un éventail quasi illimité d'objectifs en vertu des dispositions générales de mise en commun de l'information de la *Loi sur les douanes*.

Ces objectifs, pour le seul compte du gouvernement, comprennent toutes les activités en passant par les enquêtes fiscales courantes aux mesures pour repérer des pédophiles ou des blanchisseurs d'argent potentiels d'après leurs habitudes de voyage.

Il s'agit là d'un fait sans précédent. Le gouvernement du Canada n'est absolument pas en droit de créer une vaste base de données pour y emmagasiner des renseignements personnels sur tous les Canadiens et Canadiennes respectueux des lois, qui sont recueillis par des tiers sans notre consentement, non pas dans le but de nous fournir des services mais tout simplement pour les avoir à sa disposition et les utiliser contre nous si les circonstances s'y prêtaient. La compilation de dossiers sur les activités privées de citoyens respectueux des lois est le genre de choses que faisait la police secrète de la Stasi dans l'ancienne Allemagne de l'Est. Ce genre d'activité n'a aucune place dans une société libre et démocratique.

L'ADRC déclare vouloir créer cette base de données à des fins « judiciaires » : au cas où surviendrait un attentat terroriste et où les coupables seraient connus, elle utiliserait cette base de données pour trouver d'éventuels complices ou associés. L'ADRC ne possède aucun mandat en vertu de la *Loi sur les douanes* de recueillir des renseignements après le fait pour cette enquête judiciaire pour la lutte contre le terrorisme.

Cependant, j'ai demandé à maintes reprises à la ministre du Revenu, M^me^ Elinor Caplan, de limiter à tout le moins l'utilisation de cette

Il est difficile d'imaginer un plus grand mépris des droits des Canadiens et de Canadiennes. Cette base de données est au point de vue juridique et au point de vue moral fautif.

base de données à cette fin exceptionnelle de lutte contre le terrorisme en l'exemptant strictement des dispositions de mise en commun de l'information que renferme la *Loi sur les douanes*. Elle a carrément refusé.

La création de cette base de données de l'ADRC n'a pas l'autorisation parlementaire. Elle contrevient à la *Loi sur la protection de la vie privée*. De plus, il y a des motifs des plus convaincants de penser qu'elle est contraire à la *Charte canadienne des droits et libertés*.

J'ai remis à la ministre Caplan et au gouvernement, et aussi diffusé publiquement, trois opinions juridiques distinctes émanant d'autorités les plus éminentes : le juge de la Cour suprême Gérard V. La Forest maintenant à la retraite, qui a rédigé la plupart des plus importantes décisions de la Cour sur les droits de la protection de la vie privée ; l'ancien sous-ministre fédéral de la Justice Roger Tassé, qui a joué un rôle clé lors de la rédaction de l'ébauche de la *Charte canadienne des droits et libertés* ; et l'honorable Marc Lalonde, ministre de la Justice très respecté du cabinet Trudeau. Ils affirment tous trois que cette base de données semble clairement transgresser la *Charte*. Cette trilogie sans précédent d'opinions s'est heurtée à une apparente indifférence.

Il est difficile d'imaginer un plus grand mépris des droits des Canadiens et de Canadiennes. Cette base de données est au point de vue juridique et au point de vue moral fautif. Si le gouvernement peut s'en tirer avec l'enregistrement et l'analyse systématique de toutes les activités de voyage à l'étranger de tous les citoyens respectueux de la loi, alors il y a de forte chance que toutes nos autres activités privées soient enregistrées dans les mêmes dossiers personnels – nos habitudes de consommation, nos opérations bancaires, nos communications, nos déplacements à l'intérieur du pays. La société *Big Brother* veillera irrévocablement sur nous.

Projet de loi C-17, *Loi sur la sécurité publique, 2002*

Dans le projet de loi C-17, *Loi sur la sécurité publique, 2002*, le gouvernement a déposé de nouveau une disposition de l'ancien projet de loi C-55, version comportant des changements mineurs, qui permettrait à la GRC et au SCRS d'avoir un accès sans restriction aux renseignements personnels, détenus par les compagnies aériennes, de tous les Canadiens et les Canadiennes voyageant sur des vols intérieurs ou internationaux.

Je n'ai soulevé aucune objection quant à la finalité première de cette disposition, article 4.82, qui vise à permettre à la GRC et au

SI LA POLICE ÉTAIT EN MESURE D'EXÉCUTER CES TÂCHES LIÉES À L'APPLICATION DU *CODE CRIMINEL* SANS CE NOUVEAU POUVOIR AVANT LE 11 SEPTEMBRE, ELLE DEVRAIT ENCORE POUVOIR Y PARVENIR MAINTENANT.

SCRS d'utiliser de tels renseignements sur les passagers aériens aux fins de contrôle antiterroriste sur le plan de la « sécurité des transports » et de la « sécurité nationale ». Cependant, je m'inquiète du fait que la GRC serait expressément habilitée à utiliser ces renseignements pour repérer toute personne à l'égard de laquelle un mandat aurait été lancé pour des infractions au *Code criminel*, qui n'aurait aucun lien avec la lutte contre le terrorisme, la sécurité des transports ou la sécurité nationale.

Les conséquences d'une telle mesure seraient d'une portée considérable. Au Canada, il est bien établi que les citoyens n'ont pas à fournir leur identité à la police à moins d'être arrêtés ou d'exercer une activité nécessitant un permis, comme la conduite d'un véhicule. Le droit à l'anonymat face à l'État est un droit fondamental en matière de protection de la vie privée. Puisque les voyageurs aériens canadiens sont tenus de faire connaître leur identité aux sociétés aériennes, et puisque l'article 4.82 donnerait à la GRC un accès sans restriction aux renseignements que les compagnies aériennes obtiennent sur leurs passagers, cela créerait un précédent d'ingérence extraordinaire – un précédent obligeant, à toutes fins utiles, les citoyens à décliner leur identité à la police.

Je suis disposé, même si je doute sérieusement de son efficacité, à admettre à titre exceptionnel qu'une telle mesure pourrait se justifier, dans la foulée du 11 septembre, aux fins limitées et précises de la sécurité de l'aviation et de la sécurité nationale en vue de contrer le terrorisme. Néanmoins, je ne parviens pas à m'expliquer pourquoi cette mesure d'auto-identification *de facto* à la police devrait s'étendre aux personnes recherchées par l'État en raison de mandats pour des infractions au *Code criminel* qui n'ont aucun lien avec la lutte contre le terrorisme. Cela équivaut à nous contraindre à avertir la police chaque fois que nous voyageons pour qu'elle puisse vérifier si nous sommes recherchés ou non.

Si la police était en mesure d'exécuter ces tâches liées à l'application du *Code criminel* sans ce nouveau pouvoir avant le 11 septembre, elle devrait encore pouvoir y parvenir maintenant.

Si nous acceptons plutôt le principe voulant que les voyageurs aériens au Canada soient maintenant contraints de par la loi à révéler leur identité à la police dans le cadre d'une vérification en fonction d'une liste de suspects recherchés, alors qu'est-ce qui empêcherait la police d'appliquer, à l'avenir, cette même logique à d'autres modes de transport? Et plus particulièrement, si de telles dispositions devaient dissuader les personnes en cause de

voyager par avion, pourquoi ne pas étendre cette même vérification aux personnes qui voyagent en train, en autocar ou à ceux qui se louent une voiture?

En fait, le précédent que créerait cette disposition pourrait éventuellement ouvrir la voie aux pratiques semblables à celles qui ont cours dans des sociétés où les agents de police montent régulièrement à bord des trains, établissent des barrages routiers ou arrêtent les gens dans la rue pour vérifier leurs cartes d'identité en vue de rechercher toute personne que l'État suspecte.

C'est pour cette raison que j'ai recommandé de modifier le projet de loi afin de supprimer toute référence à des mandats, ce qui aura pour effet de limiter le pouvoir policier à utiliser ces renseignements sur des voyageurs aériens uniquement dans le but de surveiller les personnes recherchées précisément pour des motifs de la lutte contre le terrorisme et de sécurité nationale.

Lorsque le gouvernement a présenté de nouveau cette loi connue comme étant le projet de loi C-17, il a apporté un certains nombre de changements, mais mes recommandations concernant l'article 4.82 ont été ignorées. Au lieu de cela, le gouvernement a effectué deux modifications qui semblent être au mieux symboliques et qui visent encore plus à tromper les Canadiens et les Canadiennes plutôt que d'apporter des solutions aux enjeux fondamentaux en question.

Le gouvernement se propose maintenant d'établir un règlement visant à limiter légèrement les mandats liés à des infractions au *Code criminel* en vertu desquels la GRC peut effectuer des recherches. Toutefois, une telle mesure ne prend aucunement en compte le principe fondamental voulant que la police ne devrait pas pouvoir recourir à un accès sans restriction aux renseignements personnels pour rechercher des personnes visées par un mandat à la suite d'une infraction n'ayant aucun lien avec la lutte contre le terrorisme.

Par ailleurs, dans le nouveau projet de loi, le gouvernement a supprimé « la recherche de personnes à l'égard desquelles un mandat a été délivré » en tant que « finalité » visant à permettre l'accès à des renseignements sur les voyageurs aériens en vertu de la loi. Or, une telle mesure est vide de sens, puisque la GRC serait toujours habilitée à comparer ces renseignements avec eux d'une banque de données de personnes assujetties à un mandat et à se prévaloir d'une telle mesure pour effectuer des arrestations.

Les hauts fonctionnaires du gouvernement m'ont répété à maintes reprises que la référence aux mandats était nécessaire, sinon, la GRC ne pourrait pas agir si elle croisait « par hasard » le noms de criminels dangereux recherchés pendant le sondage d'une liste de passagers pour y trouver des terroristes possibles. Cet argument est très peu convaincant pour deux raisons.

En premier lieu, si les agents de la GRC doivent examiner les renseignements concernant les passagers dans le seul but d'intercepter des terroristes et d'évaluer les risques de sécurité, ils ne devraient pas essayer de comparer les noms des passagers avec la vaste base de données générale du CIPC, qui comprend un large éventail de renseignements dont le nom des personnes recherchées en vertu de différents mandats n'ayant aucun lien avec la lutte contre le terrorisme. Ils devraient plutôt comparer les noms avec une base de données beaucoup plus spécifique, qui se limite uniquement aux renseignements sur les présumés terroristes ou les terroristes connus ainsi que les autres personnes reconnues comme présentant un risque pour la sécurité.

Affirmer que le fait « d'aller à la pêche » au CIPC pourrait faire en sorte que la GRC identifie « à l'occasion » des personnes recherchées en vertu d'un mandat pour des infractions au *Code criminel*, c'est dire qu'il y a quelque chose « d'accidentel » dans le fait de jeter une ligne à pêche dans un étang rempli de truites et d'y pêcher une truite.

En second lieu, mes conseillers juridiques ont confirmé que les agents de la paix, notamment les membres de la GRC, possèdent des pouvoirs bien établis qui leur sont conférés par la *common law* – qui en réalité correspond à un devoir – pour prendre les mesures nécessaires pour appréhender toute personne potentiellement dangereuse qui est recherchée en vertu d'un mandat. La référence aux mandats à l'article 4.82 du projet de loi C-17 est par conséquent un peu redondante et non nécessaire – à moins, naturellement, que la GRC ne décide de faire de la recherche d'information sur des passagers pour trouver les personnes recherchées en vertu de mandats non exécutés une pratique systématique, contrairement à la fin convenue de leur donner accès à ces renseignements.

L'initiative « Accès légal »

En vertu des propositions « d'Accès légal » mises de l'avant conjointement par le ministre de la Justice, le solliciteur général et le ministre de l'Industrie, les activités dans Internet et les communications par téléphone cellulaire des Canadiens et Canadiennes respectueux de la loi pourraient faire l'objet d'examens détaillés sans précédent par l'État.

L'INTERCEPTION ET LA SURVEILLANCE DES COMMUNICATIONS PRIVÉES CONSTITUENT UNE ACTIVITÉ HAUTEMENT ENVAHISSANTE QUI FRAPPE AU COEUR MÊME DU DROIT À LA VIE PRIVÉE.

J'ai répondu de façon officielle, publique et en détail à ces propositions, par conséquent je ne le ferai pas de nouveau ici. Néanmoins, je n'ai reçu aucune indication voulant que le gouvernement ait pris en considération les préoccupations critiques concernant la protection de la vie privée que j'ai exprimées. De plus, j'ai de bonnes raisons de croire que le gouvernement à l'intention d'aller de l'avant.

L'interception et la surveillance des communications privées constituent une activité hautement envahissante qui frappe au cœur même du droit à la vie privée. Si les Canadiens et les Canadiennes ne peuvent plus être assurés que leurs activités d'internautes et leurs communications électroniques sont réellement privées, le droit à la vie privée que défend notre pays sera gravement dépouillé, et ce, de manière inutile et injustifiable.

Le gouvernement n'a présenté aucune preuve pour démontrer la nécessité des nouvelles ingérences massives qu'il propose.

Je reconnais que les nouvelles technologies de l'information et des communications peuvent constituer un enjeu de taille en ce qui concerne les techniques conventionnelles d'interception et de surveillance utilisées par les services de police et les organismes de sécurité nationale. Il semble raisonnable d'affirmer que les organismes d'application de la loi et de sécurité nationale devraient posséder la même capacité d'interception et de surveillance des communications par courriel et par téléphone cellulaire, avec le même type d'autorité judiciaire fondée sur les mêmes critères qui s'appliquent actuellement aux communications par lettre postale et par téléphone conventionnel.

Néanmoins, les agents de l'État au Canada ne peuvent demander à la Société canadienne des postes de photocopier l'adresse figurant sur chaque enveloppe que nous expédions, ni aux librairies de conserver un registre de tous les livres que nous achetons, et encore moins de toutes les pages de toutes les revues que nous feuilletons. Il n'y a aucune raison de pouvoir exercer de tels pouvoirs en ce qui concerne tous les courriels que quelqu'un envoie ou tous les sites Web qu'il consulte.

Je ne vois pas pourquoi les courriels devraient être assujettis à une norme de protection de la vie privée inférieure à celle qui s'applique aux appels téléphoniques ou à la correspondance. Et je ne vois pas non plus pourquoi le furetage dans Internet devrait être assujetti à une norme de protection de la vie privée inférieure à celle qui s'applique à l'achat de livres ou aux recherches dans des ouvrages de référence. Les Canadiens et les Canadiennes ne devraient pas être plus surveillés seulement parce qu'ils choisissent de se servir des nouvelles technologies de communication.

JE NE PEUX TROUVER AUCUNE JUSTIFICATION POUR L'ÉTABLISSEMENT D'UNE CARTE D'IDENTITÉ NATIONALE, SURTOUT PARCE QU'ELLE EST TOTALEMENT INUTILE COMME MESURE DE LUTTE CONTRE LE TERRORISME.

Dans une société libre et démocratique comme le Canada, l'interception et la surveillance des communications privées comportent des conséquences symboliques et psychologiques extraordinairement lourdes, outre celles, d'ordre plus pratique, qui sont évidentes. L'augmentation radicale de l'interception et de la surveillance sans aucune démonstration claire de leur nécessité ou de leur justification est inacceptable.

Cartes d'identité

C'est dans un état de consternation totale que le ministre de la Citoyenneté et de l'Immigration, Denis Coderre, demande avec empressement, soi-disant au nom du gouvernement, un « débat » sur l'établissement d'une carte d'identité nationale obligatoire complète, avec identification biométrique, pour tous les Canadiens et les Canadiennes.

Compte tenu du comportement actuel du gouvernement à l'égard des questions sur la protection de la vie privée, il est difficile d'éviter de craindre le pire en pensant qu'il souhaite introduire une telle carte.

Cela représenterait une autre décharge sur les droits à la protection de la vie privée. Au Canada, les personnes ne sont pas obligées d'avoir sur elles des pièces d'identité – encore moins de s'identifier sur demande – à moins de pratiquer une activité autorisée, telle que la conduite automobile. L'introduction d'une carte d'identification nationale, même « facultative » au début, nous pousserait vers une société où les agents de police pourraient arrêter n'importe qui sur les voies publiques et demander : « Vos papiers, s'il vous plaît. »

Le concept voulant que le gouvernement du Canada puisse obtenir les empreintes digitales et rétiniennes de tous les citoyens est d'autant plus déplorable, car il n'a que pour seul but celui d'établir une telle carte.

Je ne peux trouver aucune justification pour l'établissement d'une carte d'identité nationale, surtout parce qu'elle est totalement inutile comme mesure de lutte contre le terrorisme. Comme l'ont démontré les auteurs des attentats du 11 septembre, les terroristes ne sont pas nécessairement identifiables avant de tels événements. Chaque citoyen serait en mesure d'obtenir et de montrer une carte d'identité, sans égard à son inclination aux activités terroristes possibles, mais il va de soi que l'occupation « terroriste » n'y serait pas inscrite. Les visiteurs de passage au Canada n'auraient pas droit à cette carte.

Au lieu de lancer un « débat » sur l'ingérence grave et inutile, le Canada a besoin d'une attestation claire de la part du gouvernement comme quoi le droit fondamental à la protection de la vie privée de l'anonymat, tel que nous le vivons chaque jour, est trop important pour être abrogé sans raison apparente.

Surveillance vidéo

Depuis plus d'un an, je m'efforce de convaincre le gouvernement d'ordonner à la GRC de cesser la surveillance vidéo constante sur une rue publique de Kelowna, en Colombie-Britannique, surveillance qui vise des citoyens parfaitement respectueux de la loi.

Je crois que la surveillance vidéo générale de nos rues et de nos places publiques, par la police ou par d'autres pouvoirs publics, constitue la plus importante menace aux droits fondamentaux de la personne à sa vie privée dans notre société.

Nous jouissons ici au Canada du droit fondamental de marcher librement dans nos rues sans être systématiquement surveillés par la police. Si nous sommes privés de ce droit, nous perdons une caractéristique fondamentale de notre vie privée et de notre liberté.

Au mois de mars dernier, j'ai demandé conseil au juge de la Cour suprême du Canada maintenant à la retraite, Gérard La Forest, qui a rédigé plusieurs des plus importantes décisions judiciaires sur les droits de la protection de la vie privée. M. La Forest m'a donc informé que, selon lui, non seulement la façon d'agir de la GRC à Kelowna constitue une grave atteinte aux droits à la vie privée, mais elle enfreint aussi clairement la *Charte canadienne des droits et libertés*.

En avril dernier, j'ai rendu cette opinion juridique publique, mais elle a également été ignorée par la GRC et le gouvernement. À titre de Commissaire à la protection de la vie privée, je suis mandaté par le Parlement afin de superviser et de défendre les droits de la protection de la vie privée des Canadiens et des Canadiennes et puisque j'ai de bonnes raisons de croire que les agissements de la GRC à Kelowna contreviennent non seulement aux droits de la protection de la vie privée en général, mais sont également inconstitutionnels, mon seul recours est donc de solliciter l'intervention des tribunaux.

Par conséquent, en juillet dernier, j'ai déposé devant la Cour suprême de la Colombie-Britannique à Kelowna, une poursuite visant à déclarer inconstitutionnelles les activités de surveillance vidéo de la GRC à Kelowna, ces activités contrevenant à la *Charte canadienne des droits et libertés* et aux ententes internationales.

Étonnamment, le gouvernement a adopté une position que cette action remettait en question mon droit à prendre une telle mesure. Le gouvernement prend position qu'en tant que Commissaire à la protection de la vie privée, je représente un « organisme créé par la loi », dont la portée d'action se limite à ce qui est expressément prévue par la *Loi sur la protection de la vie privée.*

Mes conseillers juridiques ont affirmé être confiants que cette position n'était pas exacte en vertu de la *Loi.* Mais j'ai de bonnes raisons de croire que si mon droit d'amorcer cette contestation en vertu de la *Charte* est accueilli par la cour, le gouvernement a l'intention de déposer une série d'appels en vue d'empêcher que ce cas important soit entendu selon son mérite pour les prochaines années à venir.

Cela serait répréhensible. Au moment où la surveillance vidéo des voies publiques devient une lubie qui attire trop de municipalités au Canada, les Canadiens et les Canadiennes ont le droit d'exiger que cette importante question concernant leurs droits à la protection de leur vie privée en vertu de la *Charte* soit statuée le plus tôt possible. De plus, les services de police et les municipalités de l'ensemble du Canada ne devraient pas être soumis à l'incertitude prolongée et inutile concernant la légalité constitutionnelle de ce qu'ils sont en train d'étudier. Ils veulent et ils ont besoin d'une décision de la cour.

Par conséquent, j'ai demandé à maintes reprises au ministre de la Justice et procureur général, M. Cauchon, de retirer cette objection de procédure et de permettre à ce cas d'être rapidement déterminé selon son mérite. J'ai récemment été informé qu'il avait refusé de le faire.

Au lieu de cela, le gouvernement, par l'entremise du ministre de la Justice, adopte la position extraordinaire que le Commissaire à la protection de la vie privée du Canada ne devrait pas avoir le droit de demander à la cour de déterminer si une ingérence grave dans la protection à la vie privée constitue une violation de la protection de la vie privée en vertu de la *Charte canadienne des droits et libertés.*

J'exhorte le gouvernement de reconsidérer cette position.

La prémisse selon laquelle « ce sont les États-Unis qui nous ont forcé la main » ne peut servir de motif suffisant ou acceptable pour que le gouvernement se permette d'enfreindre un droit fondamental des Canadiens et des Canadiennes.

En ce qui concerne toutes ces initiatives, à part la surveillance vidéo des voies publiques, les représentants du gouvernement m'ont à maintes reprises affirmé que les pressions exercées par le gouvernement des États-Unis sont un important facteur de motivation.

Permettez-moi d'être direct : La prémisse selon laquelle « ce sont les États-Unis qui nous ont forcé la main » ne peut servir de motif suffisant ou acceptable pour que le gouvernement se permette d'enfreindre un droit fondamental des Canadiens et des Canadiennes.

Le Canada est un pays souverain.

Tout au long de notre histoire, il y a eu des circonstances importantes où le Canada a jugé nécessaire d'afficher une position différente de celle des États-Unis sur des questions relatives aux droits ou aux valeurs. Il n'est certainement pas exagéré de dire que si nos dirigeants avaient, de fait, constamment succombé aux pressions des États-Unis pour adopter les approches de ce pays et les faire nôtres, il n'y aurait plus, de nos jours, le Canada distinct que nous connaissons.

Il en va de même du respect approprié des droits fondamentaux, au lendemain des événements du 11 septembre. S'il est vrai que le gouvernement américain exerce des pressions sur le Canada pour qu'il prenne des mesures qui ne peuvent être justifiées selon leurs propres mérites en regard de nos valeurs canadiennes, ainsi que de nos droits, alors les Canadiens et les Canadiennes sont en droit de s'attendre à ce que le gouvernement tienne fermement à s'acquitter de ses responsabilités plutôt que de piétiner les droits des citoyens par crainte de représailles de la part du gouvernement américain.

Les Canadiens et les Canadiennes sont également en droit de s'attendre à ce que le gouvernement réfléchisse attentivement et de façon éclairée avant d'accepter la prémisse des États-Unis selon laquelle nous sommes tous « en guerre » contre le terrorisme et qu'il est par conséquent raisonnable d'imposer des restrictions en temps de guerre sur la protection de la vie privée et sur les autres droits.

La difficulté réside dans le fait que le terrorisme n'est pas notre ennemi, mais un phénomène. Les guerres déclarées entre les États-nations, ou même les guerres civiles déclarées au sein d'un pays, sont significatives. Elles peuvent durer une éternité, mais en bout de ligne il y a toujours un vainqueur et un perdant ou elles peuvent parfois se terminer sans issue, alors les conditions de paix sont établies.

Mais si nous appliquons les prémisses de guerre aux défis engendrés par le terrorisme, par définition nous nous engageons dans une « guerre » sans fin – puisqu'il n'existe aucun ennemi définissable. N'importe quel groupe de personnes ou même une personne seule qui est prête à commettre du grabuge sur un lieu public pour soutenir une cause particulière est un terroriste. Aussitôt qu'un groupe particulier ou qu'une faction de terroristes est neutralisé, un autre groupe est prêt à faire surface.

Par conséquent, cela signifie qu'en aucun moment il ne sera possible de déclarer une victoire définitive dans une « guerre » contre le terrorisme. En fait, une telle guerre évoque sinistrement l'œuvre de George Orwell, *1984*, dont la toile de fond représente une guerre chronique inexplicable dans laquelle il est impossible de déterminer qui est l'ennemi ou qui est le vainqueur ou le vaincu.

Nous devons reconnaître par conséquent, que toute ingérence ou toutes les limites sur les droits fondamentaux de la personne en matière de protection de la vie privée imposées comme des soi-disant mesures en temps de guerre pour la lutte contre le terrorisme ne seront probablement jamais annulées. Nous faisons actuellement face à la perspective d'une redéfinition complète de notre société.

Que réalisera cette redéfinition relativement à notre protection?

En fait, la réalité montre qu'il n'existe aucune mesure de sécurité qui peut garantir une protection complète contre des assassins prêts à perdre leur propre vie pour arriver à leur fin. Même les régimes autoritaires les plus répressifs n'ont pas été en mesure de se protéger complètement contre le terrorisme. Cependant, nous devons garder les risques en perspective : dans tous les scénarios possibles, les Canadiens et les Canadiennes sont plus susceptibles d'être victimes d'un accident de la route que d'un attentat terroriste.

Je ne suggère pas ici de prendre une approche cavalière en ce qui concerne le terrorisme, mais que nous devons prendre une approche plus équilibrée.

Lorsque les gens craignent pour leur sécurité, lorsqu'on a vu les horreurs dont est capable la nouvelle race de terroristes – et il y en aura peut-être d'autres – il est facile de perdre toute perspective des choses. Il est facile de tomber dans le piège et de penser que la sécurité est tout ce qui compte et que les droits de la personne tels que la vie privée sont un luxe.

Cependant, de tels extrêmes ne peuvent que récompenser et encourager le terrorisme plutôt que de le diminuer. Ils ne peuvent que dévaster nos vies sans les protéger de façon proportionnelle.

Nous devons aussi nous prémunir contre l'empressement des organes d'application de la loi et autres organismes de l'État à se servir de la réaction au 11 septembre comme d'un cheval de Troie pour acquérir de nouveaux pouvoirs envahissants.

Il est certain que nous tenons tous à être en sécurité. Mais nous pourrions – peut-être – mieux nous protéger contre le terrorisme si nous évacuions de façon permanente tous les gratte-ciel, en arrêtant nos métros, en clouant au sol, et pour toujours, tous nos avions.

Et pourtant, aucune personne saine d'esprit ne serait susceptible de prôner de telles mesures. Nous dirions « Oui, nous voulons être en sécurité – mais pas au prix du sacrifice de tout un mode de vie ».

Le même raisonnement devrait s'appliquer, à mon avis, aux arguments voulant que le droit à la vie privée devrait être sacrifié sans discrimination sur l'autel de la sécurité accrue.

L'objet même du terrorisme réside dans les répercussions qu'il vise à avoir sur ceux qui en sont témoins – la capacité d'effrayer, de démoraliser, de saper la volonté d'une société de résister à quoi que ce soit, c'est cela que cherchent les terroristes.

Dans le cas des attentats terroristes du 11 septembre, au dire de tous, c'est la nature même de la société américaine et, par voie de conséquence, de toutes les sociétés occidentales, qu'il cherche à attaquer et à saper. Nos libertés et nos valeurs, dont, c'est certain, notre droit à la vie privée, sont précisément au centre de cette cible.

Afin de faire en sorte que cela ne devienne pas une réalité au Canada, nous devons prendre garde de devenir la proie de l'illusion que l'érosion en bloc du droit à la vie privée est un moyen raisonnable, nécessaire ou efficace d'accroître la sécurité.

Nous devons nous protéger contre la tendance qu'a démontré le gouvernement de créer de nouvelles bases de données transgressant le droit à la vie privée en s'appuyant sur la nécessité légitime et exceptionnelle d'accroître la sécurité, puis de tenter d'utiliser ces renseignements pour toute une gamme d'autres objectifs d'application de la loi ou d'ordre public qui n'ont rien à voir avec la lutte contre le terrorisme – tout simplement parce qu'ils existent.

Nous devons aussi nous prémunir contre l'empressement des organes d'application de la loi et autres organismes de l'État à se servir de la réaction au 11 septembre comme d'un cheval de Troie pour acquérir de nouveaux pouvoirs envahissants ou abolir les mesures de protection établies tout simplement parce que cela fait leur affaire.

Peut-être sera-t-il nécessaire d'accepter certaines des nouvelles mesures envahissantes pour accroître la sécurité. Mais ces choix doivent être faits calmement, minutieusement et au cas par cas. Le fardeau de la preuve doit immanquablement reposer sur ceux qui laissent entendre qu'il faut de nouvelles mesures d'incursion dans la vie privée ou de restriction de ce droit au nom de la sécurité.

J'ai suggéré que toute mesure proposée en ce sens doit passer un test en quatre volets :

Il doit être possible de démontrer sa nécessité pour répondre à un besoin précis.

Il faut pouvoir faire la preuve qu'elle est susceptible d'être efficace pour atteindre le but visé. En d'autres mots, elle doit être susceptible de nous rendre plus en sécurité, pas juste de nous faire ressentir plus en sécurité.

L'atteinte à la vie privée doit être proportionnelle à l'avantage qui en découlera sur le plan de la sécurité.

Et enfin, il faut faire la preuve qu'aucune autre mesure moins envahissante ne pourra permettre d'atteindre les mêmes objectifs.

Nécessité, efficacité, proportionnalité, et absence d'autre solution plus respectueuse de la vie privée – c'est le test en quatre volets qui, selon moi, nous permettra de prendre les mesures appropriées pour accroître la sécurité sans y sacrifier inutilement le droit à la vie privée. C'est un test sur lequel nous devrions tous – chaque Canadien et Canadienne, et surtout chaque député et sénateur, de chacun des partis et de toutes les philosophies politiques – résolument insister.

L'une des leçons les plus claires que nous ait donné l'histoire est que les plus grandes menaces contre la liberté ne viennent pas quand les temps sont sereins et que tout va bien, mais en période de tumulte, lorsque la fidélité aux valeurs et aux principes semble être un luxe qu'on peut difficilement se permettre. L'histoire nous enseigne aussi que lorsque nous avons cédé à ce genre de point de vue, nous avons toute une vie pour le regretter.

Sur le coup, la perte de liberté semble mince, et même futile, à côté de la sécurité que nous cherchons à obtenir. Et pourtant, ces menaces graduelles sont celles que nous devons mettre le plus de vigilance à contrer. Le penseur politique du 18e siècle, Edmund Burke, connaissait ce danger, quand il a écrit [traduction] « Le danger réel existe lorsque la liberté est sapée, par opportunisme, petit à petit ».

Le juge Thurgood Marshall, de la Cour suprême des États-Unis a exprimé avec éloquence ce même point de vue plus récemment en déclarant [traduction] : « L'histoire enseigne que les graves menaces contre la liberté surgissent souvent en des situations d'urgence, quand il apparaît extravagant de vouloir défendre les droits constitutionnels. »

Nous vivons actuellement ce genre d'époque. Le Canada a, au cours de son histoire, établi un équilibre très sain entre les pouvoirs de l'État et les droits des personnes. Nos taux de criminalité ont toujours été relativement faibles et notre ordre social a toujours été très

fort, tandis que la liberté et la diversité des personnes ont connu un essor jusqu'à un niveau qui fait l'envie de bien des pays dans le monde. C'est d'ailleurs pour cette raison que de nombreux immigrants provenant de diverses sociétés ont choisi le Canada comme pays d'adoption.

Par contre, nous devons maintenant faire face aux contrecoups de l'équilibre que nous avons réussi à atteindre, en voyant le Canada se transformer en une société où l'État s'immisce de plus en plus dans la vie privée des gens et où les droits et les libertés de la personne sont de ce fait réduits. De plus, nous devons affronter cette transformation sans en effectuer d'analyse, en débattre ou même en assurer la compréhension qu'elle mérite.

Malheureusement, la plupart des ministres qui prennent ces décisions ne réfléchissent pas suffisamment aux répercussions profondes de leurs actions. Bien que j'essaie de maintenir le dialogue avec les fonctionnaires responsables pour arriver à apporter les changements nécessaires, au moment de l'impression du présent rapport, aucun progrès évident n'avait encore été fait.

Même avec l'aide et le soutien de mes collègues provinciaux et territoriaux, des autres défenseurs de la vie privée et des nombreux membres sérieux de la presse – à tous ceux dont je suis profondément reconnaissant – en ma qualité d'ombudsman, je n'ai pas le pouvoir d'arrêter les attaques sans précédent du gouvernement sur la protection de la vie privée.

Ce pouvoir, seuls l'insistance du Parlement et les protestations du public peuvent l'exercer. J'espère sincèrement que ce pouvoir sera exercé de toute urgence. J'espère également, même s'il est déjà un peu tard, que le gouvernement aura le courage et le bon sens de reconnaître qu'il n'y a aucune honte à repenser et à réviser des politiques qui n'ont pas suffisamment été examinées. Par contre, il est honteux d'uniquement insister au lieu de piétiner inutilement les droits fondamentaux des Canadiens et des Canadiennes.

En ce qui me concerne, mon rôle et ma responsabilité consistent à être témoin de ce qui arrive et de lutter avec tous les moyens dont je dispose. Je continuerai de le faire sans relâche et de toutes mes forces.

Première partie
Rapport concernant la *Loi sur la protection des renseignements personnels*

Introduction

La *Loi sur la protection des renseignements personnels* assure la protection de la vie privée des individus en ce qui concerne des renseignements personnels détenus par les institutions fédérales.

La *Loi*, qui est entrée en vigueur en 1983, régit les moyens pris par les institutions fédérales pour recueillir, utiliser, communiquer et retirer des renseignements personnels, et accorde aux individus le droit d'accéder à leurs renseignements personnels et de demander des corrections au besoin.

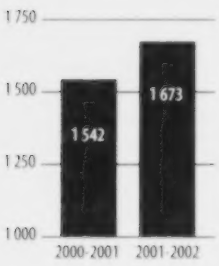
À titre de Commissaire à la protection de la vie privée, je reçois des plaintes d'individus qui croient que leurs droits aux termes de la *Loi* ont été violés et je fais enquête sur ces plaintes. Je peux également prendre l'initiative d'une plainte et faire enquête moi-même concernant toute situation pour laquelle j'ai des motifs raisonnables de croire que la *Loi* a été enfreinte.

Je suis avant tout un ombudsman, et je tâche dans la mesure du possible de résoudre les plaintes par la médiation et la négociation. Mais je possède également de vastes pouvoirs d'enquête qui me sont conférés par la *Loi*. À titre de Commissaire à la protection de la vie privée, je peux assigner des témoins à comparaître et à témoigner, et je peux pénétrer dans des locaux afin d'obtenir des

documents et de tenir des entrevues. L'entrave aux enquêtes est une infraction à la *Loi*. Bien que la *Loi* ne prévoie pas de pouvoirs en vue de contraindre à la conformité, je peux recommander aux institutions fédérales de modifier les processus qu'elles emploient pour traiter les renseignements personnels, suivant mes conclusions.

Enquêtes sur les plaintes terminées

1er avril 2001 - 31 mars 2002



En outre, je suis investi du mandat de mener des vérifications périodiques des institutions fédérales afin de déterminer leur niveau de conformité avec la *Loi* et, suivant mes conclusions, je peux recommander des changements.

Aux termes de la *Loi*, je suis tenu de déposer un rapport annuel au Parlement sur les activités de l'exercice antérieur du Commissariat. Le présent rapport vise la période du 1er avril 2001 au 31 mars 2002 au titre de la *Loi sur la protection des renseignements personnels*.

Enquêtes

La Direction des enquêtes mène des enquêtes sur les plaintes déposées par des individus aux termes de l'article 29 de la *Loi sur la protection des renseignements personnels*, ainsi qu'aux termes de l'article 11 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, dont il sera question ci-après dans le rapport.

Par le biais de ces enquêtes, je détermine si les droits à la vie privée des individus ont été violés ou si ces derniers ont pu avoir accès convenablement à leurs renseignements personnels. Lorsque les droits à la vie privée d'individus ont été violés, je leur offre des mesures de recours et j'envisage des façons pour empêcher que les violations se reproduisent.

Je suis également autorisé aux termes de la *Loi* à faire prêter serment, à recevoir les éléments de preuve et à pénétrer dans des locaux le cas échéant. Je peux également examiner ou me faire remettre des exemplaires de documents trouvés dans n'importe quel local.

Jusqu'à présent, nous avons obtenu des collaborations volontaires et toutes les plaintes déposées en vertu de la *Loi sur la protection des renseignements personnels* ont été résolues sans que nous n'ayons à invoquer ces pouvoirs d'enquête officiels.

PLAINTES EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Durant l'exercice allant du 1er avril 2001 au 31 mars 2002, nous avons reçu au total 1 213 plaintes en vertu de la *Loi sur la protection des renseignements personnels* (la *Loi*). Quarante-cinq pour cent de ces plaintes concernaient un refus d'accès à des renseignements personnels, 20 % portaient sur des questions de collecte, d'utilisation, de divulgation, de conservation et de retrait des renseignements personnels, et les 35 % qui restent portaient sur le défaut de répondre à une demande d'accès dans les délais prescrits par la *Loi*.

Le personnel d'enquête a mené à terme des enquêtes touchant 1 673 plaintes, soit une augmentation de 8 % par rapport à l'exercice précédent. Parmi celles-ci, 703 se rapportaient au refus d'accès, 397 se rapportaient aux questions liées à la collecte, à l'utilisation, à la communication, à la conservation et au retrait des renseignements personnels, 571 concernaient le défaut de répondre dans les délais aux demandes d'accès aux renseignements personnels et deux concernaient d'autres questions, notamment une allégation au sujet de représailles à l'endroit d'un individu pour avoir soumis une demande d'accès. Les décisions relativement aux plaintes ont été rendues comme suit :

Non fondées :	445
Fondées :	668
Fondées et résolues :	91
Résolues :	26
Résolues en cours d'enquête :	344
Abandonnées :	99

Définition de conclusions aux termes de la *Loi sur la protection des renseignements personnels*

Non fondée : Lorsqu'une plainte est jugée *non fondée*, cela signifie que l'enquête n'a relevé aucun élément de preuve qui me porte à conclure que l'institution fédérale n'a pas respecté les droits d'un plaignant aux termes de la *Loi sur la protection des renseignements personnels*.

Fondée : Lorsqu'une plainte est jugée *fondée*, cela signifie que l'institution fédérale n'a pas respecté les droits d'un individu relatifs à la *Loi sur la protection des renseignements personnels*. Ce serait également ma conclusion dans une situation où l'institution fédérale refuse d'accorder l'accès à des renseignements personnels malgré ma recommandation que ceux-ci soient communiqués. En pareil cas, la prochaine étape pourrait consister à demander un recours en révision à la Cour fédérale du Canada.

Fondée-résolue : Je conclus qu'une plainte est *fondée et résolue* lorsque les allégations sont corroborées par l'enquête et que l'institution fédérale a accepté volontairement de prendre des mesures correctives pour remédier à la situation.

Résolue : Il s'agit d'une conclusion officielle qui reflète mon rôle d'ombudsman. Cette conclusion est réservée aux plaintes pour lesquelles une conclusion *fondée* serait trop sévère dans les cas de mauvaise communication ou de malentendu. Cela signifie que le Commissariat, après avoir mené une enquête complète et minutieuse, a permis de négocier une solution qui satisfait toutes les parties.

Résolue en cours d'enquête : Il ne s'agit pas d'une conclusion officielle, mais d'une façon acceptable de résoudre une plainte. Une fois que l'enquête est terminée, le plaignant est satisfait des efforts déployés par le Commissariat et il consent à laisser tomber l'affaire. Le plaignant retient toutefois le droit de demander qu'une conclusion officielle soit rendue. Le cas échéant, l'enquêteur rouvre le dossier et dépose un rapport officiel. Je fais alors rapport sur les conclusions dans une lettre au plaignant.

Abandonnée : Il s'agit d'une enquête qui est terminée avant que toutes les allégations ne soient pleinement examinées. Une affaire peut être *abandonnée* pour un certain nombre de raisons, par exemple, le plaignant peut ne plus vouloir donner suite à l'affaire ou il est impossible de lui demander de fournir des renseignements supplémentaires, qui sont essentiels pour en arriver à une conclusion. Je ne dépose pas de conclusion officielle lorsqu'une plainte est abandonnée.

Dans mon rapport de l'an dernier, j'ai émis des réserves à l'égard de certains ministères et organismes fédéraux, notamment le Service correctionnel du Canada (SCC), le ministère de la Défense nationale (MDN), l'Agence des douanes et du revenu du Canada (ADRC) et Développement des ressources humaines Canada (DRHC), qui avaient fait preuve de laxisme en ne répondant pas aux demandes d'accès en temps opportun.

Il semble que ces ministères et organismes améliorent leurs délais de réponse, car ils ont pris des mesures spéciales visant à combler leurs arriérés. L'an dernier, nous avons reçu moins de plaintes relatives aux délais de réponse à l'endroit de ces institutions, à l'exception du MDN. Cela peut dénoter un rendement amélioré ou simplement le fait qu'ils ont reçu moins de demandes l'an dernier. C'est pourquoi, moins d'individus insatisfaits se sont adressés au Commissariat pour obtenir de l'aide. Néanmoins, la majorité des plaintes relatives aux délais de réponse à l'égard du SCC, du MDN et de DRHC, pour lesquelles nous avons mené une enquête, ont été jugées fondées, ce qui montre clairement que ces institutions ne remplissent toujours pas leurs obligations aux termes de la *Loi sur la protection des renseignements personnels*.

SOMMAIRE DE CAS CHOISIS EN VERTU DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Les ministères sont responsables des renseignements recueillis en vertu d'un marché

Malgré les rappels, certains ministères négligent de s'assurer que les renseignements personnels recueillis en vertu d'un marché négocié avec des entrepreneurs de l'extérieur sont gérés conformément aux principes liés aux pratiques équitables en matière de renseignements qui sont énoncés dans la *Loi sur la protection des renseignements personnels*.

Suivant ces principes, les institutions fédérales, qui sont visées par la *Loi*, sont tenues d'inclure dans les contrats des mentions qui :

- précisent la propriété des renseignements – c'est-à-dire que tous les renseignements recueillis en vertu du marché sont la propriété du ministère ou de l'organisme contractant et qu'ils doivent lui être remis à la cessation du marché ;
- reconnaissent les droits d'accès des individus à leurs renseignements personnels qui sont recueillis en vertu du marché ;
- restreignent les utilisations ultérieures des renseignements personnels ;

- protègent les renseignements contre toute communication non autorisée ;
- établissent les critères en matière de conservation et de retrait ; et
- assurent la capacité du ministère à vérifier la conformité des pratiques de gestion des renseignements des entrepreneurs.

Dans une enquête menée l'an dernier, une employée de Développement des ressources humaines Canada (DRHC) s'est plainte qu'elle n'avait pas obtenu tous les renseignements personnels la concernant qu'avait recueillis une entrepreneuse indépendante engagée par le Ministère pour évaluer le milieu de travail. Plus particulièrement, l'employée voulait avoir accès à tout renseignement la concernant qu'auraient mentionné d'autres membres du personnel, et qui serait contenu dans les notes d'entrevue et les questionnaires de l'entrepreneuse.

Lorsqu'elle a été interviewée, l'entrepreneuse a reconnu avoir détruit tous les renseignements, sauf le rapport qu'elle avait présenté à DRHC. Elle a dit avoir fait cela en partie parce qu'elle avait assuré aux individus qu'elle avait interviewés, que leurs déclarations demeuraient confidentielles. Elle a précisé que le contrat qu'elle avait signé avec DRHC ne portait pas d'indication contraire.

Bien que les politiques et procédures de DRHC relatives à l'impartition à des tiers précisent que toutes les dispositions de la *Loi sur la protection des renseignements personnels* doivent être respectées, l'entrepreneuse dans cette affaire n'était pas au courant des obligations de DRHC relatives à la conservation des renseignements ou au droit des individus à consulter les renseignements les concernant, obligations qui sont prévues par la *Loi*. En effet, il faut informer les entrepreneurs (ainsi que les employés qui mènent des enquêtes administratives similaires) qu'ils ne peuvent assurer la confidentialité et, avant de recueillir des déclarations sur un individu donné, ils doivent aviser les témoins que leurs déclarations constituent les renseignements personnels d'autres individus qui sont visés par des droits d'accès dans la *Loi sur la protection des renseignements personnels*. Les témoins peuvent alors décider de faire ou non une déclaration qui comprendrait des renseignements sur un autre individu.

J'ai conclu que la plainte était fondée et DRHC était responsable des travaux réalisés en vertu du marché. Le fait que l'entrepreneuse n'a pas conservé les renseignements a essentiellement entraîné l'impossibilité pour la plaignante de consulter les renseignements la concernant.

Dans une affaire impliquant le ministère de la Défense nationale, un officier m'a demandé de l'aider à obtenir l'accès à ses dossiers médicaux, notamment les notes d'un spécialiste médical indépendant que le Ministère avait engagé pour formuler un avis à son sujet à l'examen

de son dossier médical. Lorsque l'officier a présenté sa demande d'accès, le Ministère lui a communiqué les documents médicaux contenu dans son dossier, mais ne lui a pas communiqué les notes du spécialiste qui avait effectué l'examen indépendant.

Lors de mon enquête sur cette affaire, j'ai appris qu'aucun effort n'avait été fait pour obtenir les renseignements du spécialiste. J'ai interviewé le spécialiste et j'ai pris connaissance de ses notes, qui renfermaient clairement des renseignements personnels sur le plaignant. Le spécialiste a indiqué qu'il n'avait pas été informé que les renseignements qu'il allait recueillir dans le cadre de son examen allait appartenir au Ministère et qu'il devait également en fournir des copies au Ministère pour qu'elles soient versées à ses dossiers. Néanmoins, le spécialiste a remis volontiers des copies des renseignements au plaignant. Le plaignant était content de les recevoir et n'a pas tenu à ce que nous poursuivions l'affaire.

Ces deux affaires mettent en lumière le fait que les ministères et organismes fédéraux, qui passent des marchés en vertu desquels des renseignements personnels sont recueillis, doivent veiller à ce que les contrats comprennent des clauses appropriées afin de satisfaire aux dispositions de la *Loi sur la protection des renseignements personnels*. Les individus devraient être en mesure d'avoir accès aux renseignements personnels les concernant lorsqu'ils le demandent.

La GRC exige des frais pour les rapports d'analyse de la circulation

Un résidant de la Colombie-Britannique a demandé à la Gendarmerie royale du Canada (GRC) de lui faire parvenir un exemplaire du rapport d'analyse de la circulation qui avait été rédigé à la suite de l'enquête sur un accident de la route dans lequel il était impliqué. L'auteur du rapport avait tenté de rétablir les circonstances entourant l'accident, et le résidant voulait s'en servir pour appuyer une poursuite civile. Lorsqu'il a présenté une demande non officielle pour obtenir un exemplaire du rapport au détachement de la GRC qui l'avait rédigé, on lui a fait comprendre qu'il devait acquitter des frais de 500 $. Il a par la suite présenté une demande officielle en vertu de la *Loi sur la protection des renseignements personnels*, mais sa demande a été refusée parce que le rapport était visé par une exemption en application de l'alinéa 22(1)*a)* de la *Loi*. L'alinéa 22(1)*a)* permet à un organisme d'enquête tel que la GRC de refuser l'accès aux renseignements concernant une enquête licite qui remonte à moins de vingt ans. Dans sa lettre de plainte, le plaignant demandait, à juste titre, pourquoi les renseignements lui seraient envoyés s'il payait les frais de 500 $, mais non en vertu d'une demande aux termes de la *Loi sur la protection des renseignements personnels*, demande qui n'est pas visée par des frais.

J'ai déterminé que la réponse du détachement de la GRC à la demande non officielle du

plaignant était fonction d'une grille de frais établis. Lorsque l'Unité de l'accès à l'information et de la protection des renseignements personnels de la GRC à Ottawa a reçu la demande en vertu de la *Loi sur la protection des renseignements personnels*, elle a indiqué que l'accident faisait toujours l'objet d'une enquête. La GRC refuse régulièrement l'accès à l'information qui se rapporte à des enquêtes courantes. L'Unité a par la suite informé le plaignant que le rapport intégral était visé par une exemption aux termes de l'alinéa 22(1)*a)* de la *Loi*.

Toutefois, après avoir poussé l'enquête plus loin, j'ai appris qu'en août 2002, la GRC avait envoyé un bulletin à tous ses détachements en Colombie-Britannique indiquant que des frais ne devaient pas être exigés pour ces rapports. Cette décision faisait suite au jugement que la Cour suprême de la Colombie-Britannique a rendu en 1998 dans une affaire mettant en cause la GRC, qui remplissait le rôle de force policière municipale dans le cadre d'un marché passé avec la province. La Cour a statué que les frais exigés par la GRC pour les rapports d'analyse de la circulation représentaient essentiellement une taxe déguisée sous forme de frais d'utilisation, et étaient ainsi sans fondement légal.

À la suite de notre intervention, la GRC a communiqué au résidant seulement les renseignements personnels le concernant, qui étaient compris dans le rapport et auxquels il avait droit en vertu de la *Loi sur la protection des renseignements personnels*.

Le MDN conserve et utilise indûment des renseignements sur des délinquants réhabilités

J'ai fait enquête sur les plaintes déposées par deux membres des Forces armées canadiennes qui croyaient que le ministère de la Défense nationale (MDN) avait violé leurs droits à la vie privée en conservant dans ses dossiers des renseignements sur leurs condamnations criminelles, qu'il avait par la suite utilisés pour leur refuser une possibilité d'emploi.

Dans la première affaire, le membre avait été choisi pour faire partie d'une délégation des Nations Unies au Moyen-Orient, mais juste avant son départ, son affectation a été annulée par le commandant de la base. J'ai appris que la police militaire du MDN avait découvert que le membre avait été accusé de conduite avec facultés affaiblies peu avant le départ prévu et elle avait examiné ses dossiers afin de déterminer si d'autres accusations avaient déjà été portées contre lui. Son dossier faisait référence à sept infractions criminelles de diverses natures, et la police militaire a transmis cette information au commandant de la base. Lorsque celui-ci a pris connaissance du dossier, il a décidé d'annuler l'affectation du membre à l'étranger.

J'ai déterminé que deux des infractions auraient dû être retirées du dossier du membre parce qu'il avait été gracié dans ces deux cas.

La Division de la clémence et des pardons de la Commission nationale des libérations conditionnelles avait avisé le MDN de ces réhabilitations et de l'obligation du Ministère, aux termes de la *Loi sur le casier judiciaire*, de séparer les dossiers renfermant ces infractions des autres dossiers judiciaires en sa possession. Le MDN s'est conformé à cette obligation, mais seulement en ce qui concerne les condamnations – tous les faits liés aux accusations qui ont entraîné ces deux condamnations sont restés au dossier.

Malheureusement, lorsque seulement les documents de référence sur une condamnation sont retirés d'un dossier, les documents restants peuvent induire en erreur toute personne qui a accès à ces renseignements. Pour ces motifs, j'ai rappelé au MDN, qu'en vertu de la *Loi sur la protection des renseignements personnels* il est tenu de s'assurer que les renseignements personnels utilisés à des fins administratives – c'est-à-dire qui ont une incidence directe sur l'individu qu'ils concernent – soient exacts, à jour et complets.

Suivant mon intervention, le MDN a convenu de modifier sa politique en matière de conservation des renseignements sur les condamnations ayant fait l'objet d'une réhabilitation, de façon à se conformer à la fois à la *Loi sur la protection des renseignements personnels* et à la *Loi sur le casier judiciaire.*

Dans la seconde affaire, un individu a pris connaissance de renseignements qui l'ont porté à croire que le MDN avait utilisé des renseignements sur ses condamnations aux termes de la *Loi sur la défense nationale* pour rejeter sa demande de réadmission dans les Forces armées canadiennes, malgré le fait qu'il avait été gracié.

Dans mon enquête sur cette affaire, j'ai confirmé que le MDN avait de fait utilisé ces renseignements pour évaluer la demande de l'individu en cause. J'ai également confirmé auprès de la Division de la clémence et des pardons de la Commission nationale des libérations conditionnelles, qu'elle avait octroyé la réhabilitation à l'individu, mais avait omis d'en informer le MDN. Pour ces motifs, j'ai demandé à la Commission nationale des libérations conditionnelles d'envoyer les avis nécessaires au MDN et aux Archives nationales, dépositaires actuels des dossiers militaires de l'individu, de façon à modifier leurs dossiers, comme il était indiqué dans les circonstances.

La demande de renseignements sur l'impôt par la SCHL est inappropriée

Le président d'une société-conseil s'est plaint que la Société canadienne d'hypothèques et de logement (SCHL) avait demandé aux propriétaires uniques et aux partenariats de fournir un nombre considérable de renseignements personnels dans le cadre d'un appel d'offres. Dans la mesure où le proposant principal était un propriétaire unique, il devait, entre autres, fournir des exemplaires de ses

déclarations de revenus pour les trois dernières années ainsi qu'un état de son avoir net.

J'ai beaucoup discuté avec la SCHL de son processus d'appel d'offres. La Société a maintenu catégoriquement qu'elle devait obtenir des renseignements financiers du proposant principal lorsque l'approvisionnement présentait des risques élevés et qu'elle devait demander des renseignements détaillés d'un propriétaire unique au même titre que tout autre entrepreneur. En ce qui a trait au propriétaire unique à l'encontre d'une société, la SCHL a soutenu qu'il y a peu de renseignements financiers détaillés qui peuvent être utilisés pour effectuer une évaluation exacte des risques, et que les renseignements demandés étaient les meilleurs et les plus fidèles qu'elle pouvait obtenir.

J'étais d'avis qu'il était nécessaire d'évaluer la viabilité financière du proposant principal afin de réduire l'exposition de l'organisation à des risques élevés. Toutefois, je ne croyais pas que, pour atteindre cet objectif, il fallait évaluer les renseignements sur l'impôt sur le revenu pour une période de trois ans. En effet, il se peut qu'un individu ait touché des revenus substantiels pendant trois ans sans que les renseignements sur l'impôt sur ses revenus indiquent comment il en a disposé. En outre, un propriétaire peut avoir connu trois années difficiles et avoir tout de même respecté ses engagements financiers dans le cadre d'un marché. Un individu peut également posséder d'importants biens immobiliers ou des placements non productifs d'intérêts qui ne sont pas indiqués dans ses documents d'impôt.

L'article 4 de la *Loi sur la protection des renseignements personnels* prévoit que les renseignements personnels recueillis par une institution fédérale doivent se rapporter directement à l'un de ses programmes ou à l'une de ses activités. Étant donné que je ne croyais pas que les renseignements sur l'impôt sur le revenu aident la SCHL à évaluer les mérites de la proposition d'appel d'offres d'un propriétaire unique, je n'ai pu conclure que la demande de ces renseignements par la SCHL satisfaisait aux exigences de l'article 4. À la suite de mon enquête, la SCHL a modifié sa politique d'approvisionnement et n'exige plus des propriétaires uniques qu'ils présentent leurs déclarations de revenus ou états de leur avoir.

Il est inadmissible que des citoyens canadiens doivent fournir des exemplaires de leurs déclarations de revenus afin de pouvoir faire affaire avec le gouvernement. Aux termes de la *Loi de l'impôt sur le revenu*, les individus doivent communiquer un nombre considérable de renseignements personnels lorsqu'ils remplissent leurs déclarations de revenus, notamment sur les membres de leur famille. Le processus même de déclaration des revenus est extrêmement indiscret, et l'utilisation des renseignements personnels recueillis pour les

besoins de l'impôt sur le revenu doit, à mon avis, être strictement limitée aux fins qui ont fait l'objet d'une réglementation. À une époque où les Canadiens et Canadiennes s'inquiètent de plus en plus de l'effritement de leur vie privée, je crois qu'il est inacceptable qu'on demande à des individus de produire leurs déclarations de revenus à des fins autres que celles qui sont prévues dans la loi. Les Canadiens et Canadiennes ne devraient jamais accepter que l'un de leurs droits fondamentaux soit brimé lorsqu'ils font affaire avec le gouvernement.

En bout de ligne, la SCHL a accepté ma conclusion et a mis fin à sa pratique. Bien que mon enquête ait essentiellement porté sur les pratiques de la SCHL, j'étais conscient que d'autres ministères et organismes fédéraux employaient des pratiques similaires. C'est pourquoi j'ai écrit à la sous-ministre de Travaux publics et Services gouvernementaux Canada, au secrétaire du Conseil du Trésor ainsi qu'au contrôleur général du Canada pour demander leur concours pour faire en sorte que cette pratique soit supprimée dans l'ensemble du gouvernement fédéral. Le Conseil du Trésor a convenu du bien-fondé de mon opinion, et a indiqué qu'une telle pratique n'était pas une politique officielle et que la question serait soulevée auprès d'autres ministères et organismes. Le ministère de Travaux publics et Services gouvernementaux Canada m'a également fait savoir qu'il supprimera cette pratique.

Surveillance indue des comptes de courrier électronique d'employés

J'ai fait enquête sur plusieurs plaintes déposées par des individus qui s'interrogeaient sur les pouvoirs des gestionnaires de faire des recherches dans les comptes de courrier électronique gouvernementaux dans le cadre d'enquêtes administratives.

Dans un cas particulier, deux employés de la Commission de l'immigration et du statut de réfugié (CISR) ont allégué que la gestion locale avait indûment extrait des copies de messages électroniques confidentiels qu'ils s'étaient envoyés relativement à une plainte en vertu de la *Loi sur la protection des renseignements personnels* que l'une des employées de la CISR avait déposée auprès du Commissariat.

Pour donner quelques faits dans cette affaire, mentionnons que l'une des employés avait relevé les évaluations du rendement de plusieurs de ses collègues sur un réseau local et avait immédiatement avisé son représentant syndical, autre employé de la CISR. Le représentant a obtenu des exemplaires des évaluations afin d'appuyer sa plainte relative à la communication inappropriée de renseignements personnels qu'il a déposée auprès du Commissariat.

Mon enquête sur cette affaire a permis d'établir que la CISR n'avait pas pris de mesures convenables afin de limiter l'accès aux renseignements, et j'ai conclu que la plainte était fondée.

La gestion de la CISR a corrigé le pépin informatique qui était à l'origine du problème, dès qu'elle a été informée de la teneur de la plainte. La gestion a également amorcé une enquête dans cette affaire afin de déterminer s'il fallait prendre des mesures disciplinaires à l'endroit de l'employée qui avait communiqué les évaluations au représentant syndical. Après avoir reçu des directives à cet égard, le gestionnaire local de la technologie de l'information a cherché puis extrait quelques messages électroniques relatifs à l'incident qu'avaient échangés l'employée et le représentant syndical.

La CISR n'avait pas adopté de politique officielle de l'utilisation des réseaux électroniques lorsque cet incident s'est produit. En l'absence d'une telle politique, la CISR doit se conformer aux politiques du Conseil du Trésor relatives aux attentes en matière de respect de la vie privée des employés et aux utilisations autorisées. La CISR a indiqué qu'elle souscrit au principe selon lequel l'accès au compte de courrier électronique d'un employé à son insu est seulement justifié dans des situations extrêmes, par exemple, en l'occurrence d'une infraction criminelle ou d'une entorse à la sécurité, et seulement sur autorisation des cadres supérieurs.

Toutefois, dans l'affaire en question, avant de faire une recherche sur le réseau électronique, la CISR était déjà au courant des mesures prises par l'employée et de sa communication avec le représentant syndical. La décision de la CISR d'extraire leurs messages électroniques ne s'appuyait pas sur leur usage indu du système. L'objet principal était plutôt pour mener une enquête disciplinaire interne.

Je suis convaincu qu'il n'était pas nécessaire que la CISR extraie les messages électroniques échangés afin de déterminer si des mesures disciplinaires devaient être prises à l'endroit de l'employée. C'est pourquoi les gestes qu'elle a posés ne sont pas justifiés aux termes de la *Loi sur la protection des renseignements personnels*. J'ai recommandé à la CISR de terminer rapidement son enquête disciplinaire et de diffuser une politique, semblable à celle du Conseil du Trésor, régissant l'utilisation de ses réseaux électroniques.

Dans une autre affaire, une employée de Développement des ressources humaines Canada (DRHC) s'est plainte que son supérieur avait extrait des messages électroniques personnels qu'elle avait transmis de la maison à une collègue, et que DRHC en avait fait un usage inapproprié dans le cadre d'une enquête interne qui portait sur des allégations que son syndicat local avait faites à l'endroit de la plaignante.

J'ai déterminé que la gestion locale de DRHC menait une enquête sur des allégations, selon lesquelles l'employée avait fait obstacle au processus de grief. Durant l'enquête, DRHC

a fait une recherche dans sa base de données sur le réseau Internet afin de relever tout message électronique qu'elle aurait transmis à une collègue particulière concernant le grief. DRHC n'a pas tâché d'obtenir le consentement de l'un ou l'autre individu avant de faire la recherche dans le compte de courrier électronique au bureau du collègue. Un message personnel de la plaignante à la collègue faisait référence à l'auteur du grief en le mentionnant de nom, mais aucun autre renseignement n'a été relevé concernant le grief. Le message était surtout de nature personnelle. Pourtant, le Ministère s'en est servi par la suite durant le processus d'enquête.

J'accepte qu'il soit justifié à l'occasion pour un employeur d'examiner le compte Internet d'un employé, et qu'il se serve des renseignements recueillis lors du processus disciplinaire. Toutefois, il ne s'agit pas d'une telle occasion. Rien ne semblait indiquer que la collègue était impliquée de quelque façon que ce soit dans l'enquête interne, ce qui aurait porté DRHC à faire une recherche dans son compte. En extrayant à leur insu les messages électroniques personnels que s'étaient échangées la plaignante et la collègue et en utilisant par la suite ces renseignements dans son enquête, DRHC a violé les droits de la plaignante relatifs à la *Loi sur la protection des renseignements personnels.*

Un homme se voit refuser l'accès à ses renseignements personnels à la suite d'une enquête sur les crimes de guerre

Un émigrant européen, depuis citoyen canadien, m'a demandé d'intervenir après que la Gendarmerie royale du Canada (GRC) lui a à maintes reprises refusé l'accès à son dossier d'enquête, qui portait sur ses activités lorsqu'il était soldat nazi dans les camps de concentration où étaient internés des Juifs durant la Deuxième Guerre mondiale.

Cet homme s'était vu refuser l'entrée aux États-Unis en 1990 parce que son nom figurait dans une base de données qui renfermait des renseignements recueillis par le Bureau des enquêtes spéciales (BES) du ministère de la Justice des États-Unis. La base de données comprenait les noms de tous les membres d'une unité nazie, quel qu'ait été leur rang, occupation ou activité. Le BES a par la suite demandé à la GRC de faire une enquête afin de déterminer la mesure dans laquelle cet homme était impliqué dans l'unité nazie. Durant l'enquête, menée conjointement par la Section des crimes de guerre de la GRC et la Section des crimes contre l'humanité et les crimes de guerre de Justice Canada, la GRC a interrogé l'homme relativement aux allégations qui avaient été faites aux États-Unis.

Pendant plusieurs années, ce dernier a tâché d'obtenir des renseignements de la GRC au sujet de l'enquête pour qu'il puisse prendre des mesures indiquées pour se disculper, mais a toujours essuyé un refus. La GRC a indiqué qu'elle poursuit toujours l'enquête sur les allégations et que toute communication des renseignements dans ses dossiers compromettrait l'intégrité de l'enquête.

Le plaignant a de nouveau demandé d'obtenir un exemplaire du dossier en 2000, après avoir reçu une lettre du ministère de la Justice qui l'avisait que l'enquête conjointe avec la GRC était terminée et que le dossier avait été fermé. De nouveau, la GRC a refusé d'accéder à sa demande, indiquant que le dossier intégral était visé par une exemption aux termes de l'alinéa 22(1)*a)* de la *Loi sur la protection des renseignements personnels*, et lui a dit de vive voix que l'enquête était toujours en cours. C'est alors qu'il a déposé une plainte au Commissariat.

Lorsqu'un agent à la protection de la vie privée de la Direction des enquêtes a examiné les renseignements que la GRC refusait de communiquer, il a noté que certains de ces renseignements dataient de plus de 60 ans et ne pouvaient donc être visés par l'exemption en application de l'alinéa mentionnée par la GRC. La GRC a ensuite envisagé d'appliquer une autre disposition d'exemption, c'est-à-dire l'alinéa 22(1)*b)*, mais pour ce faire, elle devait démontrer le préjudice que subirait vraisemblablement son enquête si les renseignements étaient communiqués. Étant donné que l'enquête était déjà terminée, l'agent à la protection de la vie privée s'est alors demandé en quoi la communication des renseignements porterait préjudice à l'enquête? La GRC a maintenu que l'enquête n'était toujours pas terminée, bien qu'aucune nouvelle activité n'ait été indiquée au dossier depuis 1997.

Après que l'agent à la protection de la vie privée a confirmé auprès de la Section des crimes contre l'humanité et des crimes de guerre du ministère de la Justice que l'affaire avait été close en raison de l'absence de preuves, la GRC a cédé et a accepté de communiquer les renseignements que renfermait son dossier.

La communication de renseignements durant un appel doit être limitée

Plusieurs individus, qui avaient interjeté appel d'une décision de Développement des ressources humaines Canada (DRHC) de récupérer un versement excédentaire de prestations d'assurance-emploi (a.-e.), se sont plaints que des renseignements personnels les concernant avaient été incorrectement communiqués durant le processus d'appel.

Les plaignants étaient au nombre de plus de 200 individus qui avaient touché des prestations d'a.-e. après avoir perdu leur emploi. Étant donné qu'ils avaient déposé un grief concernant leur licenciement, pour lequel ils avaient obtenu des indemnités de cessation d'emploi, DRHC a intenté une action en vue de récupérer les prestations d'a.-e. que les individus avaient touchées lorsqu'ils étaient couverts par les indemnités de cessation d'emploi. Ils ont interjeté appel de la décision de DRHC au Conseil arbitral de l'a.-e.

Dans le cadre du processus d'appel, le bureau local de DRHC a envoyé des documents à communiquer à chacun des appelants. Chaque ensemble de documents renfermait des renseignements liés à l'appel d'un individu particulier. Toutefois, l'ensemble de documents d'un plaignant comprenait un document qui renfermait les noms, adresses, numéros de téléphone et numéros d'assurance sociale (NAS) de 14 autres individus en cause. Lorsque le plaignant a informé DRHC de cette irrégularité, le ministère a passé en revue ses dossiers et a déterminé que deux appelants seulement avaient reçu ce document.

DRHC a immédiatement pris des mesures pour récupérer le document auprès des deux individus et l'a remplacé par un exemplaire dûment vérifié. Il a également communiqué par téléphone ou lettre avec les autres personnes dont les renseignements personnels avaient été communiqués par inadvertance et pour expliquer l'erreur.

Après que les plaignants n'ont pas obtenu gain de cause dans l'appel, ils ont tâché d'obtenir un examen de deuxième niveau, pour lequel le bureau de district de DRHC devait envoyer à chaque appelant des documents à communiquer qui se rapportaient directement à lui. De nouveau, l'un des plaignants a reçu les mêmes documents qu'auparavant, qui renfermaient des renseignements personnels de 14 autres appelants. C'est cette seconde communication qui a poussé le plaignant à déposer une plainte au Commissaire.

J'étais inquiet à l'idée que le bureau de district de DRHC communique les mêmes renseignements que ceux du bureau local, malgré le fait qu'il a admis que la communication était erronée. De toute évidence, le bureau local aurait dû au départ vérifier convenablement le document avant de le transmettre. Cette erreur a été aggravée lorsque le bureau de district a envoyé les mêmes renseignements une seconde fois, ce qu'il a cru devoir faire par souci d'équité procédurale. J'ai conclu que DRHC avait violé les droits du plaignant aux termes de la *Loi sur la protection des renseignements personnels*.

Pour ces motifs, j'ai recommandé à DRHC d'adopter des procédures en vue d'assurer l'équité procédurale à toutes les étapes du processus d'appel touchant l'a.-e. et, en même temps, de tenir compte de ses obligations aux termes de la *Loi sur la protection des renseignements personnels* qui consistent à communiquer seulement les renseignements personnels qui se rapportent directement à l'appel en cause.

Dans une autre affaire, une femme s'est plainte que l'information qu'elle avait fournie à DRHC pour appuyer sa demande de prestations au survivant, en vertu du *Régime de pensions du Canada*, a été communiquée à des membres de la famille de son conjoint de fait décédé. DRHC avait obtenu une demande à la fois de la plaignante et de l'épouse légitime du défunt, et a finalement accordé les prestations à la conjointe de fait. L'épouse légitime a interjeté l'appel de la décision de DRHC auprès du bureau du Commissaire des tribunaux de révision (OCRT).

DRHC est tenu, aux termes des *Règles de procédure des tribunaux de révision*, de transmettre à l'OCRT des exemplaires de tous les documents qui sont pertinents pour ses décisions. Aux termes des *Règles*, l'OCRT doit remettre des exemplaires de ces documents à l'appelant. Pour ces motifs, l'OCRT a transmis des exemplaires de tous les documents que lui a fait parvenir la conjointe de fait du défunt. Ces documents renfermaient des renseignements que la conjointe de fait avait fait parvenir à DRHC pour démontrer sa relation avec le défunt et son droit aux prestations – notamment son NAS, sa demande de prestations de la Sécurité de la vieillesse, une copie du titre de propriété et des renseignements sur un compte bancaire conjoint.

La communication des renseignements par DRHC à l'OCRT ne contrevenait pas aux dispositions de la *Loi sur la protection des renseignements personnels* – cette communication a été faite conformément à un règlement qui autorise une telle communication, en vertu d'une loi du Parlement. De plus, l'OCRT n'est pas visé par la *Loi sur la protection des renseignements personnels*. Néanmoins j'étais inquiet à l'idée que l'OCRT ait obtenu plus de renseignements de DRHC que ce qui était nécessaire dans les faits. Certains renseignements, tels que le NAS de la conjointe de fait et des détails sur son compte bancaire, n'étaient pas essentiels à la décision de DRHC, et n'auraient pas dû être partagés avec l'OCRT pour les besoins de l'appel. En réponse à mes inquiétudes, DRHC a accepté de revoir au cas par cas les documents qu'il entend remettre à l'OCRT, en tenant compte des droits à la vie privée de tous les individus en cause, tout en fournissant suffisamment de renseignements afin d'assurer la tenue d'une audience équitable et complète.

La Société canadienne des postes modifie sa position concernant le recours au consentement négatif pour vendre des adresses aux expéditeurs de courrier grand public

Le Commissariat a reçu une plainte, selon laquelle la Société canadienne des postes, société d'État, utilisait et communiquait indûment des renseignements personnels qu'elle recueillait dans le cadre de son service du Programme national sur les changements d'adresse (PNCA). Le plaignant a indiqué que la Société canadienne des postes vendait les nouvelles adresses des abonnés aux expéditeurs de courrier grand public et aux entreprises de marketing direct, à moins que les abonnés communiquent avec la Société par écrit pour demander spécifiquement que leurs renseignements ne soient pas communiqués à cette fin. Une telle pratique est appelée « un consentement négatif », que les Canadiens et Canadiennes ont pris en grippe par le passé.

Pour obtenir ce service, les individus versent des frais à Société canadienne des postes, de façon à faire réacheminer leur courrier jusqu'à ce qu'ils aient l'occasion d'aviser leurs correspondants de leur changement d'adresse. Pour s'abonner, ils doivent signer un Avis de changement d'adresse (ACA) qui renferme l'autorisation suivante :

> […] Je reconnais que l'information fournie servira à la livraison du courrier à ma nouvelle adresse. Je reconnais également que la Société canadienne des postes peut donner ma nouvelle adresse aux expéditeurs de courrier qui en font la demande, à condition qu'ils connaissent déjà mon nom au complet et mon ancienne adresse.

En signant cette autorisation, les individus demandaient à la Société canadienne des postes d'exécuter le service particulier qu'ils avaient acquitté, c.-à-d. réacheminer leur courrier à leur nouvelle adresse. Toutefois, ils acceptaient également quelque chose qu'ils n'avaient pas demandé précisément – permettre à la Société canadienne des postes de vendre leur nouvelle adresse à des expéditeurs de courrier grand public et à des entreprises de marketing direct – à moins, tel qu'il est indiqué au verso du formulaire, qu'ils écrivent dans les sept jours à la Société pour lui demander de ne pas le faire.

De nombreux individus peuvent avoir lu ce passage sans se rendre compte que « donner » signifiait vendre et qu'« expéditeur de courrier » signifiait *n'importe quel* expéditeur, essentiellement les entreprises qui vendent du pollupostage.

J'ai fait part à la Société canadienne des postes de mon inquiétude, à savoir que les abonnés ne se rendaient pas compte qu'ils consentaient à ce que leurs renseignements personnels soient transmis à des expéditeurs de courrier grand public lorsqu'ils signaient l'ACA. Selon

la Société canadienne des postes, les abonnés signifiaient leur consentement lorsqu'ils signaient le formulaire, et ils pouvaient aviser la Société s'ils ne voulaient pas que leur nouvelle adresse soit transmise à tous les expéditeurs. J'ai fait remarquer à la Société canadienne des postes que pour l'empêcher de vendre leurs renseignements personnels à des expéditeurs de courrier grand public, les abonnés devaient lire les petits caractères au recto de l'ACA, qui les renvoyaient à d'autres détails au verso, où il était indiqué : « La Société canadienne des postes transmettra sans frais supplémentaires votre nouvelle adresse permanente aux entreprises et organismes qui en font la demande ».

Je ne partage pas l'avis de la Société canadienne des postes, selon lequel elle avait de fait obtenu un consentement. Non seulement la notion de « consentement négatif » ne tient-elle pas suffisamment compte des droits à la vie privée des Canadiens et Canadiennes, mais la Société canadienne des postes n'a dans les faits pas obtenu de consentement. Aux termes de la *Loi sur la protection des renseignements personnels*, une organisation ne peut prétendre avoir votre consentement si elle n'a pas indiqué ce à quoi vous consentez.

Ce qui était réellement en cause, c'était la notion de consentement éclairé. Le paragraphe 5(2) de la *Loi* oblige une institution fédérale à vous informer des fins auxquelles elle recueille des renseignements personnels vous concernant. La Société canadienne des postes informait-elle les abonnés au service du PNCA des fins visées de façon suffisamment claire et précise? Est-ce qu'une personne raisonnable, à la lecture de l'ACA, comprendrait qu'elle consent à ce que ses renseignements personnels soient vendus à des expéditeurs de courrier grand public et à des entreprises de marketing direct? Je suis certain qu'elle ne le saurait pas. En ce qui concerne le consentement, les attentes raisonnables des individus sont aussi pertinentes.

A priori, la Société canadienne des postes a convenu de donner suite à certaines de mes recommandations de façon à rendre le service du PNCA plus transparent et respectueux des droits à la vie privée. Elle a accepté de remplacer le mot « reconnaissance » par « autorisation » au recto de l'ACA et d'ajouter la mention « notamment les expéditeurs de publipostage ». Toutefois, la Société canadienne des postes a été peu disposée à accepter ma principale recommandation : donner aux abonnés au service un choix positif en ajoutant une case à cocher au recto du formulaire. La Société canadienne des postes était d'avis qu'un tel ajout minerait le service du PNCA et entrainerait des frustrations et des inconvénients pour ses clients.

J'ai convaincu la Société canadienne des postes du contraire. En effet, j'ai soutenu que celle-ci bénéficierait d'un tel ajout, car ses clients apprécieraient le fait qu'elle fait tout ce qu'elle peut pour protéger leurs droits à la vie privée et que ces derniers en tireraient également parti. Les clients qui veulent recevoir des envois des expéditeurs de courrier grand public peuvent clairement indiquer leur choix, tandis que ceux qui ne veulent pas de pollupostage peuvent également indiquer leur choix. En bout de ligne, ce serait les clients qui auraient le choix, et non la Société canadienne des postes.

La Société canadienne des postes a finalement accepté d'ajouter une case à cocher sur le consentement positif au formulaire ACA.

INCIDENTS VISÉS PAR *LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS*

Le personnel de la Direction des enquêtes se renseigne sur les incidents qui ont été portés à mon attention par des sources variées, mais qui ne sont pas considérés comme des plaintes officielles aux termes de la *Loi sur la protection des renseignements personnels*. Bon nombre de ces incidents concernent la gestion (ou la mauvaise gestion) des renseignements personnels, c'est-à-dire des communications par inadvertance à des tiers, ou encore des fichiers et blocs-notes électroniques perdus ou volés. Des exemples suivent.

Communication inappropriée du NAS sur les formulaires de prestations fiscales canadiennes pour enfants

Dans une affaire particulière, un quotidien a signalé que l'Agence des douanes et du revenu du Canada (ADRC) avait accidentellement divulgué des renseignements sur des individus dans l'ouest du Canada qui touchaient des prestations fiscales canadiennes pour enfants (PFCE). Lorsque nous nous sommes penchés sur cette affaire, nous avons appris que certains contribuables recevaient les premier et deuxième feuillets de leur Avis de détermination ainsi que le troisième feuillet qui renfermait des renseignements sur un autre contribuable, c'est-à-dire le numéro d'assurance sociale (NAS), le prénom du conjoint le cas échéant, et le calendrier des versements au cours de l'année.

Même si le nom du contribuable n'était pas indiqué, le numéro d'assurance sociale est un numéro unique assigné à ce contribuable et représente ainsi un renseignement personnel, tel que défini dans la *Loi sur la protection des renseignements personnels*. Heureusement, et contrairement à ce que le quotidien a signalé, les renseignements ne comprenaient pas le nom de famille, l'adresse du domicile, le nom des enfants et leur date de naissance, ou encore le revenu familial de l'autre contribuable. Néanmoins, nous avons tous entendu des histoires de ce qui arrive lorsque les NAS

tombent entre les mauvaises mains et tous les inconvénients que cela peut entraîner dans la vie d'une personne.

L'ADRC a également mené sa propre enquête et a déterminé que le problème découlait d'une erreur de synchronisation à l'impression, probablement en raison d'un pépin informatique. Afin de prévenir un problème similaire à l'avenir, l'ADRC a modifié ses systèmes de façon à pouvoir relever toute anomalie dans la fonction de tri de l'imprimante et de la mettre hors tension. Une intervention de l'opérateur est alors nécessaire pour poursuivre l'impression, après qu'une inspection minutieuse a été effectuée. Suite à cet incident, l'ADRC a décidé qu'il n'est plus nécessaire d'imprimer le numéro d'assurance sociale sur le formulaire des prestations fiscales canadiennes pour enfants (PFCE) sur la deuxième page et les pages subséquentes.

Des documents du registre des armes à feu trouvés dans un conteneur

Plusieurs jours avant Noël, un homme a communiqué avec le Commissariat pour signaler qu'il avait trouvé trois sacs contenant des renseignements personnels, qui appartenaient au Programme canadien des armes à feu, dans un conteneur qui se trouvait dans une enceinte verrouillée de l'entreprise privée où il travaillait.

Des enquêteurs se sont immédiatement rendus sur les lieux. L'entreprise n'était pas située à proximité du Centre du traitement des demandes du programme canadien des armes à feu et le conteneur recevait strictement des produits en bois. Après examen, mes enquêteurs ont retiré un nombre d'enveloppes expédiées au Programme canadien des armes à feu, dont la majorité portaient le nom et l'adresse de l'expéditeur.

Mes enquêteurs ont confirmé qu'à l'automne, le Programme canadien des armes à feu avait envoyé une trousse contenant des demandes d'enregistrement personnalisées à tous les propriétaires d'armes à feu, ainsi que les enveloppes-réponse à l'adresse du Programme canadien des armes à feu. Les documents qu'ils ont trouvés dans le conteneur étaient les enveloppes-réponse qui avaient été renvoyées au Programme canadien des armes à feu.

Après avoir déterminé que les renseignements provenaient du Bureau canadien d'enregistrement des armes à feu, les enquêteurs ont tâché d'établir comment ces documents étaient parvenus dans l'enceinte d'une entreprise privée. Ces derniers ont confirmé que le conteneur avait été loué d'une entreprise de gestion des déchets et qu'il se trouvait dans l'enceinte depuis le début de décembre.

Mes enquêteurs ont remarqué que les sacs qui se trouvaient dans le conteneur étaient couverts de glace et qu'ils étaient collés au

fond du conteneur. Il est fort probable que lorsque l'entreprise de gestion des déchets a récupéré le conteneur de l'emplacement antérieur et l'a vidé, que les sacs y sont restés.

Mes fonctionnaires ont communiqué avec le ministère de la Justice, institution fédérale chargée du Programme d'enregistrement des armes à feu. Ses représentants ont indiqué que le Ministère avait donné en sous-traitance le traitement des formulaires d'enregistrement des armes à feu à une entreprise privée. Une réunion a alors été organisée entre les représentants du ministère de la Justice et les dirigeants de l'entreprise. Ces derniers ont depuis été pleinement renseignés sur les dispositions de la *Loi sur la protection des renseignements personnels*, et ils croyaient qu'ils avaient pris toutes les mesures de précaution nécessaires afin d'assurer le respect des droits à la vie privée des individus. Toutefois, les dirigeants de l'entreprise ont confirmé qu'ils avaient l'habitude de jeter les enveloppes-réponse dans une poubelle ordinaire, sans se rendre compte que les propriétaires d'armes à feu avaient indiqué leurs nom et adresse de renvoi sur l'enveloppe, et pouvaient ainsi être facilement identifiables en tant que propriétaires d'armes à feu. L'entreprise a alors immédiatement convenu de ne plus jeter les enveloppes avec les ordures ordinaires et a entrepris de les éliminer en employant une manière sécurisée, c'est-à-dire le déchiquetage.

DRHC et l'ADRC partagent des données sur l'admissibilité au Supplément de revenu garanti

Je me suis particulièrement intéressé à une autre affaire qui avait été hautement médiatisée – l'incapacité apparente de Développement des ressources humaines Canada (DRHC) de partager des renseignements avec l'Agence des douanes et du revenu du Canada (ADRC) en vue d'identifier les personnes âgées admissibles au Supplément de revenu garanti (SRG). Le SRG est une composante de la Sécurité de la vieillesse (SV), qui est accordé aux personnes âgées dans la tranche de revenu inférieur. Environ 1,5 million de personnes âgées touchent le SRG. Bien que cette affaire n'ait pas mis en cause directement la *Loi sur la protection des renseignements personnels*, je ne voulais pas que la législation de la protection de la vie privée ou le Commissariat soient perçus comme un obstacle aux activités des ministères fédéraux qui sont avantageuses pour les Canadiens et Canadiennes.

L'ADRC détient des renseignements des contribuables qui lui permettent de déterminer les personnes âgées admissibles au SRG, mais celle-ci avait refusé de faire connaître leur identité à la Direction générale des programmes de la sécurité du revenu de DRHC, qui accorde les prestations, en raison des dispositions relatives à la confidentialité aux termes de la *Loi de l'impôt sur le revenu*. À

mon avis, la *Loi de l'impôt sur le revenu* autorise spécifiquement la communication de renseignements personnels pour les besoins de l'administration la *Loi sur la sécurité de la vieillesse*, comme je l'ai indiqué lors de ma comparution devant le Comité de la Chambre des communes chargé de ce dossier.

Suivant les reportages dans les médias sur le manque de collaboration entre ceux des organismes fédéraux, le Commissariat a rencontré des fonctionnaires de DRHC et de l'ADRC afin de solutionner le problème, de façon que les personnes âgées qui sont admissibles au SRG soient informées du fait qu'elles peuvent toucher ce supplément du revenu. Leurs efforts ont découlé sur ce qui suit :

- L'ADRC a ajouté une page dans le guide de l'impôt de 2001 à l'intention des personnes âgées à faible revenu, qui comprend des messages clés sur le SRG et les modalités de demande ;
- L'ADRC enverra des renseignements sur la SV et le SRG aux personnes de plus de 65 ans qui ont un revenu faible ou modeste ; et
- DRHC recevra de l'ADRC la liste des personnes âgées à faible revenu qui touchent la SV mais non le SRG. En utilisant les données sur le revenu fournies par l'ADRC et les renseignements personnels existants tirés du formulaire de demande de la SV, DRHC enverra aux personnes éventuellement admissibles un formulaire de demande simplifié du SRG, qui comprendra leurs nom, adresse et les renseignements sur leur revenu pré-imprimés. Ces personnes devront confirmer ou corriger les renseignements qui figurent sur le formulaire, de façon que leur admissibilité au SRG puisse être déterminée à l'étude du formulaire par DRHC.

Je crois comprendre que DRHC et l'ADRC ont convenu de rationaliser le processus pour que les fondements juridiques soient en place, de façon à ce que les personnes âgées puissent être renseignées sur leurs droits aux prestations. Mon personnel et moi-même demeurerons à la disposition des deux organismes afin de discuter d'autres initiatives et de leur venir en aide de quelque façon que ce soit pour éviter des répercussions négatives relativement à la protection de la vie privée.

Communications dans l'intérêt public

L'alinéa 8(2)*m)* de la *Loi sur la protection des renseignements personnels* autorise les dirigeants d'une institution fédérale à communiquer des renseignements personnels dans l'intérêt public, sans le consentement explicite des individus concernés – soit parce que la communication l'emporte largement sur toute invasion corrélative à la vie privée, soit parce qu'elle serait bénéfique à l'individu auquel les renseignements se rapportent. Cette disposition a été établie afin de composer avec les situations où une institution fédérale ne peut invoquer une autre disposition énoncée au paragraphe 8(2) de la *Loi* afin de justifier la communication. Le paragraphe 8(5) de la *Loi* impose un devoir obligatoire aux dirigeants d'institution fédérale, à savoir qu'ils doivent aviser le Commissaire à la protection de la vie privée par écrit de toute communication de renseignements personnels dans l'intérêt public. L'avis doit être transmis au préalable, à moins que la situation pour laquelle la communication s'impose est si urgente que le fait de ne pas communiquer immédiatement les renseignements entraîne des préjudices précis.

L'an dernier, j'ai examiné 57 avis de communication de renseignements personnels dans l'intérêt public. Près de la moitié ont été produits par le Service correctionnel du Canada (SCC). Le SCC reçoit des demandes de tiers, notamment de groupes d'aide aux victimes, qui veulent obtenir les rapports de la Commission d'enquête qui portent sur des questions hautement médiatisées, dont des évasions de prison et des actes criminels avec violence qu'ont commis des délinquants toujours sous la surveillance du SCC. Il reçoit également des demandes de renseignements de membres de la famille de délinquants qui sont décédés alors qu'ils étaient sous la surveillance du SCC. La disposition touchant la communication dans l'intérêt public, comprise dans la *Loi sur la protection des renseignements personnels*, est la seule qui autorise le SCC à communiquer des renseignements personnels aux membres de la famille pour des motifs humanitaires, de façon que ceux-ci puissent mieux comprendre ce qui est arrivé à leur proche et les aider à vivre leur deuil.

J'ai également passé en revue les circonstances qui ont entouré l'avis que m'a fait parvenir la GRC sur son intention de communiquer aux médias des renseignements personnels d'un criminel condamné. Les médias voulaient avoir accès à un enregistrement vidéo qui avait été déposé à titre de preuve lors du procès du délinquant, en vue de produire un reportage sur l'affaire hautement médiatisée dans laquelle ce criminel était impliqué. Les médias ont fait appel à la GRC après avoir appris que la Cour avait détruit sa copie de la vidéocassette – la Cour ne conserve pas indéfiniment tous les éléments de preuve ou les pièces à conviction qui sont déposés durant les procédures. La seule copie existante se trouvait entre les mains de la GRC.

Je n'ai pas compris comment l'intérêt public serait servi en communiquant ces renseignements dans les circonstances, et j'ai demandé à la GRC de reconsidérer sa position. Bien que la vidéocassette ait été utilisée à titre de preuve dans la procédure criminelle, qui est de nature publique, il s'agissait avant tout de renseignements personnels concernant un individu identifiable qui ont été versés aux dossiers d'enquête de la GRC, qui ne sont pas habituellement mis à la disposition du public. Pour ces motifs, j'ai recommandé à la GRC de refuser la requête des médias. La GRC s'est conformée à mes recommandations.

Dix premiers ministères selon le nombre de plaintes reçues
1er avril 2001 - 31 mars 2002

Organisation	Total	Accès aux renseignements personnels	Délais	Atteinte à la vie privée	Autre
Agence des douanes et du revenu du Canada	307	152	85	69	1
Service correctionnel Canada	265	84	125	56	0
Développement des ressources humaines Canada	117	42	57	18	0
Citoyenneté et Immigration Canada	103	57	40	6	0
Gendarmerie royale du Canada	89	65	16	8	0
Défense nationale	78	31	35	11	1
Commission de l'immigration et du statut de réfugié	41	6	29	6	0
Société canadienne des postes	32	12	6	14	0
Ministère de la Justice Canada	22	6	5	11	0
Centre canadien du renseignement de sécurité	18	18	0	0	0
Autres	141	67	30	44	0
Total	**1 213**	**540**	**428**	**243**	**2**

Enquêtes terminées et résultats selon le ministère ou l'organisme

1er avril 2001 - 31 mars 2002

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Agriculture et Agroalimentaire Canada	0	0	1	1	0	0	2
Agence de promotion économique du Canada atlantique	0	0	0	0	0	2	2
Banque du Canada	0	0	0	0	0	3	3
Agence des douanes et du revenu du Canada	44	20	120	8	10	63	265
Société canadienne d'hypothèques et de logement	1	0	0	0	0	0	1
Société canadienne des postes	5	7	10	2	2	16	42
Agence canadienne d'évaluation environnementale	0	0	2	0	0	0	2
Commission canadienne des grains	0	1	0	0	0	2	3
Patrimoine canadien	0	0	1	0	0	1	2
Commission canadienne des droits de la personne	0	0	2	0	0	1	3
Société du Musée canadien des civilisations	1	0	0	0	0	0	1
Commission canadienne de sûreté nucléaire	0	0	0	0	0	3	3
Conseil de la radiodiffusion et des télécommunications canadiennes	0	0	1	0	0	1	2
Service canadien du renseignement de sécurité	0	0	35	1	0	1	37
Agence spatiale canadienne	3	1	1	1	0	0	6
Citoyenneté et Immigration Canada	40	4	26	11	0	17	98
Commission des plaintes du public contre la GRC	1	2	4	0	0	1	8

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)
1er avril 2001 - 31 mars 2002

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Enquêteur correctionnel Canada	1	0	0	0	0	0	1
Service correctionnel Canada	344	11	47	17	1	89	509
Environnement Canada	2	0	1	0	0	1	4
Financement agricole Canada	0	3	1	0	0	1	5
Pêches et Océans Canada	0	0	1	0	0	0	1
Affaires étrangères et Commerce international Canada	24	0	4	0	0	1	29
Santé Canada	0	0	0	2	0	4	6
Développement des ressources humaines Canada	86	10	45	24	2	36	203
Commission de l'immigration et du statut de réfugié	29	1	3	0	0	6	39
Affaires indiennes et du Nord Canada	1	1	9	1	1	0	13
Industrie Canada	1	0	4	1	1	2	9
Ministère de la Justice Canada	8	1	12	4	1	8	34
Archives nationales du Canada	1	0	3	1	0	5	10
Défense nationale	44	14	20	8	3	25	114
Musée des beaux-arts du Canada	0	0	0	0	0	1	1
Commission nationale des libérations conditionnelles	0	3	9	3	0	5	20
Ressources naturelles Canada	0	0	1	0	0	1	2
Bureau du directeur général des élections	0	1	1	0	1	2	5
Commissariat aux langues officielles	0	0	0	1	0	0	1
Bureau du surintendant des institutions financières	0	0	1	0	0	0	1

Enquêtes terminées et résultats selon le ministère ou l'organisme (suite)
1er avril 2001 - 31 mars 2002

Organisation	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Bureau de l'Ombudsman, Défense nationale et Forces canadiennes	1	0	1	0	0	0	2
Bureau du Conseil privé	3	1	0	0	0	0	4
Commission de la fonction publique du Canada	1	2	0	0	0	2	5
Commission des relations de travail dans la fonction publique	0	0	1	0	0	0	1
Travaux publics et Services gouvernementaux Canada	1	0	1	2	0	6	10
Gendarmerie royale du Canada	20	6	66	10	3	36	141
Solliciteur général Canada	2	0	2	0	0	0	4
Statistique Canada	3	0	2	0	0	0	5
Condition féminine Canada	0	0	2	0	0	0	2
Administration portuaire de Toronto	1	0	0	0	0	0	1
Transports Canada	0	2	1	0	0	0	3
Secrétariat du Conseil du Trésor du Canada	0	0	3	0	0	0	3
Anciens Combattants Canada	0	0	1	1	1	1	4
Diversification de l'économie de l'Ouest Canada	0	0	0	0	0	1	1
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1 673**

Enquêtes terminées selon les motifs et les résultats
1er avril 2001 - 31 mars 2002

	Fondée	Fondée et résolue	Non fondée	Abandonnée	Résolue	Résolue en cours d'enquête	Total
Accès aux renseignements personnels	**22**	**80**	**260**	**60**	**22**	**259**	**703**
Accès	22	77	249	53	22	248	671
Correction-annotation	0	3	9	4	0	4	20
Langue	0	0	1	3	0	4	8
Frais inexacts	0	0	1	0	0	3	4
Atteinte à la vie privée	**184**	**11**	**99**	**26**	**4**	**73**	**397**
Collecte	10	2	26	2	0	19	59
Conservation et retrait	10	2	5	1	1	7	26
Utilisation et communication	164	7	68	23	3	47	312
Délais	**462**	**0**	**85**	**13**	**0**	**11**	**571**
Corrections-délais	4	0	0	1	0	1	6
Délais	440	0	53	9	0	9	511
Avis de prorogation	18	0	32	3	0	1	54
Autres	**0**	**0**	**1**	**0**	**0**	**1**	**2**
Total	**668**	**91**	**445**	**99**	**26**	**344**	**1 673**

Lieu d'origine des enquêtes terminées

1er avril 2001 - 31 mars 2002

Province / Territoire	Nombre
Terre-Neuve	3
Île-du-Prince-Édouard	4
Nouvelle-Écosse	57
Nouveau-Brunswick	60
Québec	257
Région de la capitale nationale – Québec	11
Région de la capitale nationale – Ontario	116
Ontario	433
Manitoba	92
Saskatchewan	39
Alberta	271
Colombie-Britannique	315
Nunavut	0
Territoires du Nord-Ouest	0
Yukon	5
Étranger	10
Total	**1 673**

Examens et pratiques en matière de vie privée

Introduction

Je suis autorisé, aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels*, à amorcer des examens de conformité, de façon aléatoire, des pratiques de traitement des renseignements personnels des institutions fédérales. Ce que cela signifie, c'est que je procède à des vérifications afin de m'assurer que les institutions se conforment aux principes de collecte, d'utilisation, de communication, de protection, de conservation et de retrait des renseignements personnels qui sont établis dans les articles 4 à 8 de la *Loi*.

Le Commissariat effectue des examens de conformité aux termes de l'article 37 depuis 1984. J'ai élargi cette fonction l'an dernier, établissant la Direction des examens et des pratiques en matière de vie privée, afin que je puisse évaluer la mesure dans laquelle les organisations se conforment aux exigences établies dans la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. (La *Loi* visant le secteur privé me confère des pouvoirs semblables en matière de vérification. Je discute des activités de vérification dans le secteur privé dans la deuxième partie du présent rapport.)

En tant qu'ombudsman, je préfère que les vérifications de la protection de la vie privée soient non conflictuelles, dans la mesure du possible. Idéalement, une vérification représente un démarche coopérative et constructive qui permet d'aborder les questions avant qu'elles ne deviennent des plaintes. Les vérifications servent aux organisations qui veulent améliorer leurs pratiques de traitement des renseignements personnels. Bien que j'aie les mêmes pouvoirs de vérifications que ceux liés aux enquêtes – c'est-à-dire assigner des témoins à comparaître, faire prêter serment, et contraindre les organisations à produire des éléments de preuve – je n'y ai recours que lorsque je n'obtiens pas de collaboration volontaire.

Mon personnel de la Direction des examens et des pratiques en matière de vie privée, en plus d'effectuer des vérifications et des examens, travaille auprès des organismes fédéraux qui cherchent à mieux comprendre les questions touchant la conformité et les implications de leurs programmes et pratiques sur la vie privée. Il est essentiel que les ministères fédéraux explorent à fond les moyens à prendre pour protéger la vie privée avant de donner suite à leurs plans, même avec les meilleures intentions qui soit, de façon à réduire les coûts et à protéger les citoyens. Sur demande, mon personnel de la Direction analyse les nouvelles propositions relatives à la gestion des

renseignements, comme les initiatives de couplage des données, la création de bases de données et les ententes de partage de renseignements avec d'autres organisations. Il s'agit d'une autre façon d'assurer que les droits à la vie privée des Canadiens et Canadiennes sont respectés.

Au cours de l'année dernière, le Commissariat a mené à terme des examens des pratiques de traitement des renseignements personnels, aux termes de l'article 37 de la *Loi sur la protection des renseignements personnels*, de la Commission canadienne de la sûreté nucléaire (CCSN) et de la Commission de l'immigration et du statut de réfugié (CISR).

L'objet de ces examens était de se renseigner sur où et comment la CCSN et la CISR traitent les renseignements personnels ; de déterminer la mesure dans laquelle leurs politiques et pratiques de gestion des renseignements personnels sont conformes aux articles 4 à 8 de la *Loi sur la protection des renseignements personnels* en ce qui a trait au respect des pratiques équitables en matière de renseignements ; et de faire part d'observations et de recommandations le cas échéant. Au terme de chaque examen, les organisations ont reçu des rapports contenant les conclusions et recommandations détaillées. J'ai récemment fait paraître des rapports d'examens de conformité à la CNSC et à la CISR, et j'attends leurs réponses aux conclusions et recommandations.

Je n'ai pas l'intention de dévoiler systématiquement les conclusions des examens, à moins que les questions mises au jour ne soient à ce point exceptionnelles qu'elles justifient la publication. Une question exceptionnelle s'est présentée dans l'examen de la CISR.

L'examen a révélé que les bureaux régionaux de Montréal, de Vancouver et de Toronto utilisaient du matériel de télévision en circuit fermé pour surveiller l'aire de réception et les salles d'attente, ainsi que les couloirs qui menaient aux salles d'audience. Dans certains cas, de l'équipement vidéo et audio avait été installé dans les salles d'audience. Lorsque l'examen de conformité a été effectué, la CISR n'avait pas adopté de politiques ou procédures écrites internes relatives à l'utilisation de matériel de surveillance électronique, et il n'y avait pas d'enseigne pour signaler aux individus qu'ils étaient sous surveillance dans les aires où ces appareils étaient installés.

Le Commissariat se souciait particulièrement des microphones cachés dans les salles d'audience du bureau régional de Montréal, dont le siège n'était pas au courant. La conduite de surveillance clandestine – que de l'équipement vidéo ou d'autres appareils d'enregistrement soient utilisés – représente une atteinte majeure des droits à la vie privée des individus et doit être justifiée comme il se

doit. Pourtant, aucune justification raisonnable n'a été donnée concernant l'installation d'un tel matériel. Les fonctionnaires de la CISR ont depuis confirmé que les microphones en question ont été retirés, et ils ont affirmé que les dispositifs d'écoute n'ont jamais été utilisés. Le Commissariat a également appris que les syndicats ont été avisés de cette affaire et que la CISR a élaboré une politique en matière de sécurité, en vertu de laquelle toutes les régions doivent présenter leurs plans de sécurité au siège aux fins d'approbation avant de le mettre en œuvre.

Le point sur le Programme canadien des armes à feu

Depuis le milieu des années 1990, le Commissariat s'est vivement intéressé au Programme canadien des armes à feu. La *Loi sur les armes à feu* est un texte législatif hautement controversé qui continue de susciter de vives émotions à la fois auprès de ses partisans et de ses détracteurs. Je continue de m'intéresser à la mise en œuvre de cette *Loi* pour une raison bien simple : le Programme canadien des armes à feu comporte la collecte et l'utilisation d'un nombre considérable de renseignements personnels de nature très délicate. La *Loi* a également une incidence directe sur plus de 2,3 millions de propriétaires d'armes à feu au Canada, qui possèdent plus de 7 millions d'armes à feu. Je reçois toujours des plaintes et des demandes de renseignements concernant divers aspects du Programme, notamment certaines qui émanent de députés fédéraux.

Le 29 août 2001, j'ai remis mon rapport, intitulé *Examen des pratiques relatives au traitement des renseignements personnels du Programme canadien des armes à feu* au ministère de la Justice et à la GRC. La 1ère partie du rapport porte sur le résumé de l'examen du Commissariat de la conformité du Programme avec les articles 4 à 8 de la *Loi sur la protection des renseignements personnels*, où le traitement des renseignements personnels est abordé. La 2e partie renferme notre évaluation sur la pertinence des questions relatives aux antécédents personnels auxquels doivent répondre les demandeurs de permis d'arme à feu et de la conformité de ces questions avec la *Loi sur la protection des renseignements personnels*. Le rapport formulait quelque 34 recommandations détaillées en vue de la prise de mesures correctives visant à atténuer l'intrusion du Programme dans la vie privée.

Aucune de mes recommandations faite au ministère de la Justice n'a encore été acceptée. Néanmoins, la GRC a convenu de donner suite à certaines de mes recommandations dans le rapport. Je suis heureux de pouvoir indiquer, à titre d'exemple, que les agents aux armes à feu partout au Canada ne jouissent plus de privilèges d'accès intégral au Système de récupération de renseignements judiciaires

(SRRJ) de la GRC, et que toutes mes recommandations relatives à l'accès sélectif au SRRJ ont été appliquées. De plus, je m'attends à ce que la GRC apporte sous peu les révisions nécessaires au Protocole d'entente, qui porte sur quatre domaines de l'informatique et de la sécurité liés au Programme des armes à feu. Ces mesures importantes permettront de resserrer le contrôle de l'accès aux renseignements personnels de nature délicate qui est utilisé par le Programme.

Bien que je ne sois pas autorisé, aux termes de la *Loi sur la protection des renseignements personnels*, à obliger le Ministère à donner suite à mes recommandations, je poursuivrai mes efforts de façon à ce qu'il prenne des mesures indiquées pour que le Programme canadien des armes à feu soit pleinement conforme à la *Loi*.

À la suite des recherches et du travail sur le terrain qui ont étayé mon rapport initial, d'autres questions ont été mises en lumière. Le Commissariat surveille toujours les questions en instance suivantes :

- Impartition – Mise en œuvre de l'entente contractuelle existante avec BDP Business Data Services Ltd., tous les aspects de l'initiative Diversification des modes d'exécution, ainsi que les pratiques actuelles relatives aux fonctions de deuxième et troisième vérifications dans le cadre de l'impartition ; et
- Toutes les ententes internationales en matière de partage de renseignements qui se rapportent au Programme canadien des armes à feu, que ce soit directement ou indirectement par le biais d'autres organismes d'application.

Mise à jour du Protocole de gestion DRHC pour le Comité d'examen des banques de données

Dans le rapport annuel de l'an dernier, j'ai décrit comment Développement des ressources humaines Canada (DRHC), en raison de pressions croissantes exercées par le public, a décidé d'abolir le Fichier longitudinal sur la main-d'œuvre et d'adopter un processus d'examen ainsi qu'un Protocole de gestion visant toutes les activités d'analyse, de recherche et d'évaluation de politiques qui comportent la connexion de banques de données distinctes. Comme je l'ai expliqué à l'époque, le processus d'examen comprendra la consultation du Commissariat afin d'évaluer ces projets.

Depuis la dernière période de rapport, le Commissariat a commenté 17 autres présentations de DRHC, notamment l'examen du Centre d'action pour l'emploi, l'évaluation non expérimentale d'enquête et de contrôle, et la mise à l'essai de projets de couplage des données probabiliste, pour n'en nommer que quelques-uns. J'ai cru qu'il serait indiqué de discuter certains des exemples de travaux que nous avons accomplis cette année en vue d'examiner et de commenter ces présentations.

Le Commissariat a élaboré un outil d'évaluation personnalisé en vue d'assurer l'examen opportun des présentations de DRHC. L'outil devrait permettre l'exhaustivité et l'uniformité de l'examen de tels projets ainsi que le respect des principes liés aux pratiques équitables en matière de renseignements, qui sont énoncés dans la *Loi sur la protection des renseignements personnels*, lors de l'examen des présentations. Bien que nous en soyons toujours aux essais de l'efficacité de l'outil, le Commissariat a obtenu des résultats positifs jusqu'à date en l'utilisant.

En examinant l'élaboration des projets de recherche de DRHC, le Commissariat permet une vérification essentielle en vue de protéger la vie privée et soulève souvent des questions plus vastes relatives à l'utilisation des renseignements personnels à des fins qui sont liées à la recherche et à l'évaluation.

À titre d'exemple, le Programme d'évaluation non expérimentale d'enquête et de contrôle (E et C) visait à déterminer les économies ainsi que la mesure dans laquelle les activités d'E et C comportent des effets dissuasifs, de façon à évaluer l'incidence à court terme de la fonction d'E et C et ainsi de mieux gérer la Direction. Pour ce faire, les agents de recherche de DRHC ont mis en correspondance les données sur les demandes de prestations d'a.-e. et les dossiers d'E et C et, en employant des méthodes statistiques précises, ont évalué la possibilité de fraude du régime d'a.-e. en fonction de caractéristiques de base, comme des facteurs démographiques, le secteur et d'autres variables. En s'appuyant sur cette analyse, les chercheurs de DRHC ont produit une équation qui peut servir à évaluer la possibilité de fraude du régime d'a.-e. relativement à d'autres demandes de prestations d'a.-e., et ainsi à déterminer l'efficacité des interventions liées à l'E et C.

Bien que les objectifs du projet d'évaluation aient été détaillés et que DRHC ait été autorisé à évaluer le programme, la présentation demeurait ambiguë en ce qui a trait à l'utilisation ultérieure de l'équation, une fois que le projet d'évaluation serait terminé. Le Commissariat s'inquiétait à l'idée que DRHC puisse éventuellement utiliser cette équation, même si celle-ci a été créée dans un contexte de recherche, pour prendre des décisions qui touchaient directement des individus, tels que le profilage systématique de toutes les demandes de prestations d'a.-e. dans le cadre d'enquêtes éventuelles, en s'appuyant seulement sur les résultats de l'équation. Étant donné que l'accès aux renseignements personnels était strictement réservé aux activités de recherche et d'évaluation, le Commissariat était d'avis que l'équation ne pourrait être utilisée dans le cadre de l'E et C à des fins administratives ou coercitives qui touchaient directement un individu particulier.

Le Commissariat a clarifié cette question auprès de DRHC, qui a confirmé qu'il n'a jamais eu l'intention de se servir de l'équation à des fins opérationnelles et, plus particulièrement, qu'il ne se servirait pas de la méthode afin d'effectuer le profilage des individus en vue d'une enquête. DRHC a effectivement établi une distinction claire entre son travail de recherche et ses activités coercitives. Bien que DRHC ait de toute évidence adopté des pratiques indiquées relativement à ce projet, l'exemple permet d'illustrer comment l'utilisation des renseignements personnels à « des fins de recherche ou d'évaluation » peut entraîner des difficultés éventuelles si elle ne fait l'objet d'un contrôle.

Il convient de signaler que le Commissariat a noté une amélioration marquée dans le niveau de détails et d'exhaustivité des présentations relatives aux projets de DRHC, pour ce qui est de la suite à donner aux inquiétudes en matière de la protection de la vie privée. Néanmoins, il y a toujours place à l'amélioration lorsqu'il s'agit de protéger la vie privée. Dans l'examen de certaines des présentations de DRHC, une lacune commune a été relevée : étant donné que que bon nombre des propositions ne sont pas au point, elles renferment des renseignements restreints sur les marchés auxquels participent des parties de l'extérieur.

Bien que DRHC ait donné certains exemples de formulations à adopter dans les contrats, celles-ci renvoient peu ou nullement à la *Loi sur la protection des renseignements personnels*. Le Commissariat a insisté sur l'importance de la protection de la vie privée dans les ententes contractuelles auprès de consultants et de tiers. Nous avons clairement stipulé que toutes les ententes contractuelles de cette sorte doivent préciser que les renseignements personnels en cause dans la recherche doivent relever du contrôle de DRHC ; que ces renseignements sont visés par les dispositions de la *Loi sur la protection des renseignements personnels* ; et que les consultants et les tiers doivent se conformer explicitement à toutes les exigences de la *Loi*.

La signification de cette clause est double. Tout d'abord, elle rend le consultant imputable au respect des mêmes normes en matière de gestion de l'information que celles qui sont en vigueur dans l'ensemble de l'administration fédérale et, en second lieu, elle veille à ce que les dispositions relatives à la tenue d'examens et d'enquêtes comprises dans la *Loi sur la protection des renseignements personnels* soient applicables et exécutoires. Bien que nous ayons bon espoir que DRHC intègre ces clauses dans ses contrats, il importe de rappeler que mon rôle consiste en partie à effectuer des examens afin de déterminer si les pratiques actuelles en matière de protection de la vie privée d'un organisme fédéral sont conformes aux principes liés aux pratiques équitables en matière de renseignements qui sont prévus dans la *Loi sur la protection des renseignements personnels*.

Devant les tribunaux

Introduction

Aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*, un individu est autorisé, à l'issue d'une enquête par le Commissaire, à déposer auprès de la Cour fédérale du Canada un recours en révision d'une décision d'une institution fédérale qui lui a refusé l'accès à ses renseignements personnels. Depuis l'entrée en vigueur de la *Loi sur la protection des renseignements personnels* en 1983, 118 recours en révision ont été déposés à la Cour fédérale. Douze ont été déposés au cours de l'exercice qui a pris fin le 31 mars 2002.

En vertu de l'article 42 de la *Loi sur la protection des renseignements personnels*, je suis autorisé à comparaître devant la Cour fédérale. Je peux déposer auprès de la Cour fédérale un recours en révision de la décision d'une institution fédérale qui a refusé l'accès à des renseignements personnels, dans la mesure où j'ai obtenu le consentement de l'individu qui a présenté la demande d'accès initiale. Je peux également comparaître devant la Cour pour le compte de l'individu qui a déposé le recours en révision aux termes de l'article 41, ou je peux comparaître, avec l'autorisation de la Cour, comme partie à une instance engagée en vertu de l'article 41.

La liste suivante n'est pas une liste exhaustive de tous les recours judiciaires en vertu de la *Loi sur la protection des renseignements personnels*, mais plutôt le sommaire des affaires auxquelles je participe activement :

Formulaires de déclaration du voyageur (Formulaire E-311)

Nous avons engagé des poursuites dans deux affaires concernant la communication de renseignements personnels par l'Agence des douanes et du revenu du Canada (ADRC) à la Commission de l'assurance-emploi du Canada (CAEC) aux fins d'un programme d'appariement des données d'enquête afin de déterminer si des personnes recevaient frauduleusement des prestations d'assurance-emploi alors qu'elles se trouvaient à l'étranger. Les renseignements personnels en question ont été tirés de formulaires de déclaration du voyageur (E-311) présentés aux douanes par des résidants canadiens revenant au Canada entre 1994 et 1996.

- *Le Commissaire à la protection de la vie privée c. Le Procureur général du Canada*
  La Cour d'appel fédérale a conclu que la communication de renseignements personnels tirés des formulaires E-311 était autorisée par l'alinéa 8(2)*b)* de la *Loi sur la protection des renseignements personnels* et de l'article 108 de la *Loi sur les douanes*, qui accorde à la ministre du Revenu national le pouvoir discrétionnaire de communiquer des renseignements recueillis par le Ministère. Dans ce cas, la Cour a conclu que la communication de

renseignements par l'ADRC à la CAEC en vertu d'un protocole d'entente régissant les conditions de la communication est autorisée. (Article 108 de la *Loi sur les douanes* a depuis été modifié par le projet de loi S-23.)

- *Contestation en vertu de la Charte*
  La Cour d'appel fédérale a conclu qu'on ne peut raisonnablement s'attendre au respect de la vie privée touchant les renseignements inscrits sur les formulaires E-311 de manière à susciter l'application de l'article 8 de la *Charte canadienne des droits et libertés*. Cette conclusion s'appuyait sur deux éléments : la nature limitée des renseignements en question, qui ne révélaient pas de détails intimes sur le mode de vie et les choix personnels de la personne, et l'utilisation limitée obligatoire dont les renseignements devaient faire l'objet.

État de la situation

Les affaires ont été entendues le 7 novembre 2001. La Cour suprême du Canada a rendu ses décisions dans les deux cas le 7 décembre 2001. Dans chaque cas, l'argumentation de la Cour d'appel fédérale a été confirmée. En ce qui concerne la contestation en vertu de la *Charte*, la Cour suprême a expressément conclu qu'on ne peut raisonnablement s'attendre au respect de la vie privée touchant les renseignements inscrits sur les formulaires E-311 et que ces renseignements ne l'emportaient pas sur le droit de la CAEC à s'assurer du respect des obligations de déclaration du programme de prestations d'assurance-emploi.

Commissaire à l'information du Canada c. Commissaire de la GRC et Commissaire à la protection de la vie privée

Une liste des affectations de quatre agents de la Gendarmerie royale du Canada (GRC) avait fait l'objet d'une demande aux termes de la *Loi sur l'accès à l'information*. Le Commissaire de la GRC a refusé de communiquer les renseignements parce qu'ils se rapportaient aux antécédents professionnels de ces individus et qu'il s'agissait ainsi de renseignements personnels aux termes de l'article 3 de la *Loi sur la protection des renseignements personnels*.

La question en litige consistait à déterminer si les renseignements pouvaient être communiqués conformément à la définition de renseignements personnels énoncée à l'alinéa *j)* de la *Loi sur la protection des renseignements personnels*, qui précise que les renseignements touchant les postes ou fonctions d'agents ou de fonctionnaires du gouvernement ne constituent pas des renseignements personnels. La question plus vaste consistait à trouver un juste équilibre entre les dispositions de la *Loi sur l'accès à l'information* et celles de la *Loi sur la protection des renseignements personnels*.

La Cour d'appel fédérale a soutenu que les renseignements en cause étaient de fait des renseignements personnels et qu'ils n'étaient pas visés par l'exemption à l'alinéa *j)*. La Cour a conclu que l'exemption ne doit pas être interprétée de façon à empêcher la communication des antécédents professionnels d'un individu.

État de la situation

Le Commissaire à l'information a été autorisé à interjeter appel de cette décision à la Cour suprême du Canada. Quant à moi, j'ai été autorisé à intervenir dans cet appel le 7 janvier 2002. L'audience a été tenue le 29 octobre 2002, à la suite de laquelle la Cour a remis la décision en délibéré.

Clayton Charles Ruby c. Solliciteur général

Le Service canadien du renseignement de sécurité (SCRS) a rejeté la demande d'accès de M. Ruby à des renseignements personnels le concernant. M. Ruby a déposé un recours en révision aux termes de l'article 41 de la *Loi sur la protection des renseignements personnels*.

Durant l'examen judiciaire, M. Ruby a soulevé certaines questions liées à la *Charte* concernant la constitutionnalité de l'article 51 de la *Loi sur la protection des renseignements personnels*. Cet article permet des audiences à huis clos (*in camera*) ou des audiences qui excluent une des parties au litige (en l'absence d'une partie) où une institution gouvernementale a invoqué les exceptions en vertu de la *Loi* relatives aux « renseignements confidentiels reçus des États étrangers » ou à la « sécurité nationale ». La Cour d'appel fédérale a décidé que ces dispositions (l'alinéa 51(2)*a)* et le paragraphe 51(3) de la *Loi sur la protection des renseignements personnels* respectivement) portaient atteinte au droit de liberté de presse, qui est protégé par l'alinéa 2*b)* de la *Charte*, mais ces dispositions étaient justifiées aux termes de l'article 1 de la *Charte*. La Cour a conclu que ces dispositions ne violaient pas le droit à la vie privée, à la liberté et à la sécurité de l'individu protégé aux termes de l'article 7 de la *Charte*.

État de la situation

M. Ruby a été autorisé à interjeter appel à la Cour suprême du Canada concernant les questions liées à la *Charte* le 18 janvier 2001. Le solliciteur général a été autorisé à procéder à un rappel incident et j'ai été autorisé à intervenir sur la question touchant l'interprétation de l'alinéa 22(1)*b)* de la *Loi sur la protection des renseignements personnels*. La Cour suprême du Canada a entendu la cause le 24 avril 2002 et la Cour a remis le prononcé de sa décision le 21 novembre 2002.

La Cour suprême a soutenu que les procédures de l'article 51 de la *Loi sur la protection des renseignements personnels* ne tombent pas en deçà du niveau d'équité requis par l'article 7 de la *Charte*. La Cour n'a pas jugé pertinent à la décision dans cette affaire de statuer sur les arguments relatifs à la vie privée soulevés par M. Ruby en vertu de l'article 7. Du point de vue du respect de la vie privée, le jugement ne change pas le *statu quo*. La disposition impérative relative au huis clos de l'article 51 contrevient néanmoins au paragraphe 2 *b)* de la *Charte*. La Cour suprême a conclu que la disposition ne pourrait se justifier en vertu de l'article 1 de la *Charte*. La disposition est inconstitutionnelle et doit être interprétée d'une manière restrictive pour ne s'appliquer qu'à ces parties de l'audience qui portent sur le fond même d'une exception. La Cour suprême a noté que la pratique judiciaire précédente en vertu de l'article 51 visait en fait à tenir l'audience publique et à entendre uniquement les discussions sur le fond de l'exception à huis clos.

En ce qui a trait au recours en appel, la Cour suprême a confirmé les conclusions qu'elle a rendues dans l'affaire *Robert Lavigne c. Commissariat aux langues officielles* sur l'interprétation de l'alinéa 22(1) *b)* de la *Loi sur la protection des renseignements personnels* (comme suit).

Robert Lavigne c. Commissariat aux langues officielles

M. Lavigne s'est vu refuser l'accès à des renseignements le concernant qui étaient compris dans des déclarations qu'avaient faites des témoins dans le cadre d'une enquête menée par le Commissariat aux langues officielles. Le Commissariat a fondé son refus de communication sur l'exemption prévue à l'alinéa 22(1)*b)* de la *Loi sur la protection des renseignements personnels*.

La Cour d'appel fédérale a soutenu que l'alinéa 22(1)*b)* ne peut être invoqué que lorsqu'il y a preuve de préjudice dans une enquête donnée. Il ne peut être invoqué après que l'enquête est terminée, et les allégations d'« effets dissuasifs » sur les enquêtes futures ne sont pas suffisantes pour appuyer un refus de communication.

État de la situation

La Commissaire aux langues officielles a été autorisée à interjeter appel à la Cour suprême du Canada le 19 avril 2001. J'ai été autorisé à intervenir à l'appui de M. Lavigne. La Cour suprême du Canada a entendu l'affaire le 17 janvier 2002 et le jugement a été rendu le 20 juin 2002.

La Cour suprême a conclu que la dérogation de l'article 22 (1) *b)* ne se limitait pas aux enquêtes en cours. Toutefois, si une institution

veut soulever la dérogation concernant le dommage aux enquêtes futures, elle doit pouvoir démontrer un lien précis et direct entre la communication des renseignements et le dommage allégué.

La Cour suprême a conclu que le Commissariat aux langues officielles n'avait pas rempli ce critère et a ordonné qu'on communique à M. Lavigne ses renseignements personnels.

Commissaire à l'information du Canada c. Ministre de Citoyenneté et Immigration Canada et Philip W. Pirie

M. Pirie s'est vu refuser l'accès à l'identité d'employés qui ont émis des vues ou des opinions à son endroit durant un examen administratif mené par Citoyenneté et Immigration Canada. Cette information n'a pas été communiquée parce qu'elle constituait des renseignements personnels de ces employés aux termes du paragraphe 19(1) de la *Loi sur l'accès à l'information.*

La Section de première instance de la Cour fédérale a conclu que l'identité des individus qui ont fait valoir leur point de vue à M. Pirie constituait des renseignements personnels les concernant et ne devrait pas être communiquée à M. Pirie.

État de la situation

Le Commissaire à l'information a déposé une demande d'appel de la décision, soutenant que l'identité des individus qui ont fait des commentaires au sujet de M. Pirie durant le processus d'examen sont des renseignements personnels le concernant, aux termes de l'alinéa *g)* de la *Loi sur la protection des enseignements personnels*, où est énoncée la définition de renseignements personnels. J'ai été autorisé à intervenir auprès de la Cour d'appel fédérale pour appuyer la position du Commissaire à l'information. La date de l'audience a été fixée au 4 juin 2002 et le jugement de la Cour a été rendu le 21 juin 2002.

La Cour d'appel fédérale partageait mon opinion et celle du Commissaire à l'information, à savoir que l'identité des personnes interviewées devait être communiquée à M. Pirie. La Cour a noté que les noms des personnes interviewées étaient de nature personnelle, tant pour M. Pirie que pour ces personnes interviewées, mais l'intérêt de l'un devait prévaloir sur les intérêts des autres. La Cour a pris en considération les intérêts public et privé et a conclu qu'ils requéraient la communication des noms à M. Pirie. Ce jugement n'est pas porté en appel en Cour suprême.

Mertie Anne Beatty et al. c. Statisticien en chef et al.

Il s'agit d'une demande récente déposée par un groupe de citoyens canadiens qui ont demandé l'accès aux relevés du recensement de 1906 pour les provinces du Manitoba, de la Saskatchewan et de l'Alberta. Les requérants ont demandé qu'une ordonnance soit décernée à l'endroit du statisticien en chef qui l'oblige à transférer les relevés du recensement de 1906 aux Archives nationales, ainsi qu'une ordonnance signifiant aux Archives nationales de rendre publics les relevés aux fins de la recherche, conformément à l'article 6 du *Règlement sur la protection des renseignements personnels.*

État de la situation

La demande a été déposée le 5 février 2002, et je suis l'un des défendeurs nommés. Tous les arguments ont à présent été soumis. La date de l'audience n'a toujours pas été fixée.

Deuxième partie
Rapport concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*

Introduction

Un an, ce n'est pas bien long dans la vie d'une loi. Sans doute que cela n'est pas assez de temps pour permettre une analyse approfondie de l'application de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*). Pourtant, en m'appuyant sur les 28 enquêtes que nous avons menées à terme en vertu de la *LPRPDÉ* en 2001, j'ai pu tirer certaines conclusions assez solides à deux égards au moins, et je crois qu'il est instructif de faire connaître ces conclusions à ce point-ci. (Lors de mon très prochain rapport annuel, je ferai état de la deuxième année de la *LPRPDÉ*.)

En particulier, des progrès considérables ont été réalisés dans l'interprétation de ce qui constitue ou non des renseignements personnels, et dans la détermination des domaines où les organisations semblent typiquement éprouver des difficultés en vue de se conformer aux exigences de la *Loi*.

La définition de renseignements personnels : de portée vaste mais non infinie

À l'article 2 de la *LPRPDÉ*, les renseignements personnels sont définis comme suit : « tout renseignement concernant un individu identifiable ». Il est prévu pour que cette définition ait un champ d'application large, et durant la première année qui a suivi l'entrée en vigueur de la *Loi*, cette définition a permis de clarifier ce champ d'application.

Plusieurs causes ont déjà occasionné des différends, à savoir si les renseignements en cause constituent les renseignements personnels du plaignant. De manière plus notable, certaines institutions ont rapidement revendiqué le statut de « propriétaires » de certains éléments d'information attribués aux clients, tels que les numéros de compte, les numéros d'identification et de cartes de crédit. L'argument habituellement soutenu est que de tels renseignements ne doivent pas être considérés comme des renseignements personnels parce qu'ils ne sont pas recueillis auprès des clients. Ainsi, étant donné qu'ils sont produits à l'interne par l'institution même, comme l'entend l'entité, ces renseignements lui appartiennent.

Pourtant, la définition énoncée à l'article 2 a été élaborée pour éviter de tels arguments. Il n'y est pas indiqué que les renseignements personnels doivent provenir de l'individu ou être recueillis auprès de lui. Elle ne se préoccupe pas non plus de qui peut ou ne peut pas détenir un droit de propriété sur ces renseignements. Il y est seulement énoncé que les renseignements sont de nature personnelle s'ils « concernent » un individu identifiable. Au bas mot, lorsqu'une institution a porté le nom d'un individu sur un document quelconque, l'institution peut difficilement soutenir que ce document ne « concerne » pas l'individu.

La définition est intentionnellement large, et dans mes conclusions, j'ai tâché de l'interpréter le plus largement possible. De façon générale, peu importe qui a produit les renseignements, ou comment, ou qui est leur « propriétaire », ou ce que sont les usages de l'entité. Si ces renseignements ont été attribués au nom d'un individu, il est fort probable que j'accepte que ce sont des renseignements personnels le concernant.

J'ai tendance à concevoir des renseignements comme personnels même s'il est fort possible que ces renseignements concernent un individu identifiable. Le cas suivant offre un bon exemple. Un diffuseur avait tâché – par inadvertance, comme il a été démontré – de recueillir des renseignements NETBIOS de l'ordinateur d'un visiteur sur son site Web. Notre enquête a révélé que, dans certaines circonstances techniques comme celles impliquant le plaignant, l'information NETBIOS pourrait être utilisée pour retracer l'adresse Internet de l'ordinateur, puis pour retracer les sites Web visités par l'utilisateur ou les mots de passe récents utilisés pour sécuriser les comptes. En raison de l'invasion possible dans la vie privée du plaignant, j'ai déterminé que les renseignements en cause étaient des renseignements personnels visés par la *LPRPDÉ*.

Mais même une définition volontairement large doit avoir des limites. Dans une affaire hautement médiatisée, j'ai souscrit à l'idée que l'article 2 n'était pas trop large pour englober tous les renseignements associés à un individu. Plus particulièrement, j'ai déterminé que les ordonnances des médecins ou

leurs habitudes de prescription ne constituent pas des renseignements personnels concernant les médecins mêmes. Une ordonnance individuelle, à mon avis, peut être révélatrice au sujet d'un patient, sans toutefois l'être de façon significative du médecin prescripteur en tant qu'individu. Je crois plutôt que c'est le processus professionnel qui a découlé sur cette prescription qui doit être envisagé comme un produit de travail, c'est-à-dire le résultat concret de l'activité professionnelle du médecin.

J'ai également estimé que l'élargissement de la définition de façon à inclure les prescriptions et les habitudes de prescription ne serait pas conforme à l'objet de la *LPRPDÉ*. L'article 3 énonce cet objet comme suit : l'équilibre entre les droits à la vie privée et le besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels pour des fins qu'une personne raisonnable considérerait comme indiquées. Je n'ai pas cru qu'il était raisonnable d'étendre la définition pour comprendre les prescriptions, car cela engloberait aussi d'autres produits du travail, tels que les avis juridiques ou les documents rédigés en cours d'emploi. En outre, je ne croyais pas qu'il était raisonnable d'étendre la définition aux habitudes de prescription, car cela viserait aussi les habitudes discernables dans d'autres genres de produits professionnels et empêcherait donc les rapports légitimes sur les habitudes de consommation.

Problèmes systémiques

Le code type sur la protection des renseignements personnels, ce n'est qu'un début

Il arrive rarement aujourd'hui qu'une organisation ne se soucie pas grandement des droits à la vie privée des individus – du moins, sur papier. Dans la majorité de leurs brochures et leurs sites Web, les entreprises professent haut et fort avoir adopté un code type sur la protection des renseignements personnels, officiellement pleinement conforme aux obligations que doit remplir l'entreprise en vertu de la *LPRPDÉ*. Toutefois, ce que montrent les enquêtes à la suite des plaintes, c'est que certaines organisations mettent plus ou moins en pratique leur code.

Un code type sur la protection des renseignements personnels est futile s'il n'est pas assorti de politiques et de procédures exhaustives et détaillées, et celles-ci en retour sont vaines à moins qu'elles soient diffusées, observées et appliquées de façon cohérente. Les violations des droits à la vie privée qui entraînent des plaintes sont souvent imputables à des problèmes ou à des manquements dans les processus ou systèmes généraux de traitement des renseignements d'une organisation. De tels problèmes sont parfois causés parce qu'une organisation n'a pas saisi les implications pratiques des principes de la *LPRPDÉ* ou qu'elle n'y a pas accordé suffisamment d'attention. Il arrive parfois également que les

problèmes découlent d'une adhésion aveugle aux pratiques traditionnelles, qui peuvent ne plus être acceptables compte tenu de la nouvelle *Loi*.

Sont énumérés ci-dessous certains des problèmes systémiques que nos enquêtes ont relevés.

Défaut de désigner un agent à la protection de la vie privée

Le principe 4.1 de l'annexe 1 de la *LPRPDE* énonce qu'une organisation doit désigner un ou plusieurs individus chargés de la conformité de l'organisation avec les principes de la *Loi*. Dans plus d'un cas, nous avons conclu que l'organisation n'avait toujours pas désigné un tel individu ou n'avait pas identifié de personne en tant qu'agent de protection de la vie privée.

Méconnaissance du traitement des demandes d'accès et des plaintes

La majorité des organisations semblent reconnaître qu'un individu a le droit d'avoir accès à ses renseignements personnels (principe 4.9) et de contester la conformité d'une organisation (principe 4.10). Toutefois, lorsque certaines organisations font l'objet d'une demande d'accès ou d'une plainte d'un individu, elles ne savent pas comment y donner suite. Il est alors très important à ce point qu'elles aient des politiques et procédures précises en place et qu'elles les appliquent minutieusement et uniformément.

Conservation trop longue ou trop courte des renseignements

La conservation est un autre principe auquel certaines organisations doivent porter plus d'attention en adoptant des lignes directrices et procédures précises. Aux termes du principe 4.5.2, une période de conservation minimale et maximale doit être établie relativement aux renseignements personnels. Les renseignements qui ont servi à une décision au sujet d'un individu doivent être conservés pendant assez de temps pour que ce dernier puisse les consulter. En vertu du principe 4.5.3, les renseignements qu'il n'est plus nécessaire de conserver à des fins précises, devraient être détruits, supprimés ou rendus anonymes.

Ce que nous avons relevé dans certains cas, c'est que des organisations détruisent les renseignements personnels trop tôt, c'est-à-dire avant que l'individu n'ait pu les consulter, ou habituellement les conservent trop longtemps, bien après qu'elles sont tenues de le faire. Dans un cas particulier, nous avons appris qu'une organisation avait l'habitude de conserver pendant une période indéfinie les renseignements qu'elle recueillait de demandeurs de cartes de crédit qu'elle avait jugés inadmissibles, et ce, pour aucune raison particulière. Nous avons également appris qu'une organisation n'avait jamais détruit de renseignements personnels qu'elle avait recueillis, parce qu'elle ne savait pas qu'elle pouvait le faire.

Non-respect des échéances

Tel qu'il est prévu à l'article 8 de la *LPRPDÉ*, j'ai déjà déterminé dans un nombre de cas que des organisations avaient de fait refusé des demandes d'accès d'individus, car elles n'avaient pas respecté le délai de réponse fixé à 30 jours. Dans la majorité des cas, toutefois, le non-respect de l'échéance était davantage attribuable à l'absence de procédures de traitement efficaces des demandes, plutôt qu'à un refus délibéré de l'organisation.

Collecte excessive de renseignements

Est-il indiqué qu'une organisation telle qu'une entreprise Internet insiste pour obtenir votre numéro d'assurance sociale (NAS)? En bref, la réponse est non. Il y a très peu d'organisations du secteur privé qui ont des raisons légitimes de demander le NAS à leurs clients (les établissements financiers ont parfois besoin du NAS, par exemple, pour pouvoir déclarer les revenus).

Mais dans une plainte notable l'an dernier, la collecte des NAS était une question centrale. Dans ce cas particulier, l'entreprise recueillait depuis un certain temps les NAS afin d'éviter de confondre les noms similaires de clients. L'entreprise ne s'était jamais demandée si cette pratique était légitime ou non, et le personnel de point de service croyait que la collecte était nécessaire. Dans ma conclusion, j'ai déterminé que la collecte de ces renseignements n'était pas nécessaire et qu'elle était arbitraire, et de toute évidence, l'entreprise avait tort d'exiger des demandeurs qu'ils produisent leur NAS afin d'obtenir des services.

Ce n'est pas le seul cas où une organisation a recueilli plus de renseignements que ce qu'elle avait réellement besoin pour ses fins légitimes. Aux termes de la *LPRPDÉ*, les organisations doivent s'assurer non seulement que les fins pour lesquelles elles recueillent des renseignements personnels sont légitimes et raisonnables, mais également que le nombre et le genre de renseignements recueillis sont nécessaires pour réaliser ces fins. L'examen des politiques et pratiques de collecte de longue date, qui n'ont pas été remises en question, est la meilleure façon pour une organisation de commencer à se conformer au principe 4.7, Limitation de la collecte de renseignements.

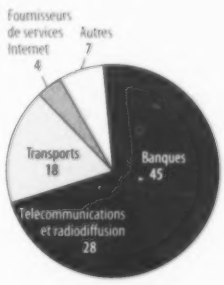
Défaut d'identifier des fins pour lesquelles les renseignements sont recueillis

Les personnes auxquelles les organisations demandent des renseignements ont le droit de savoir pourquoi. Il n'est donc pas suffisant que les fins soient légitimes, elles doivent également être signalées.

En vertu du principe 4.2, une organisation doit indiquer les fins pour lesquelles elle recueille des renseignements. Aux termes du principe 4.2.1, ces fins doivent être documentées. Aux termes du principe 4.2.3, l'organisation doit préciser ces fins à l'individu au moment de recueillir les renseignements

Nombre de plaintes selon le secteur

1er janvier 2001 – le 31 décembre 2001



ou avant de le faire. Enfin, suivant le principe 4.2.5, il incombe à l'organisation de s'assurer que les employés chargés de la collecte peuvent expliquer les fins aux individus qui s'interrogent sur la pratique.

Plusieurs plaintes déposées jusqu'à présent ont mis en lumière les violations de l'un ou l'autre de ces principes. De nouveau, dans certains cas, la raison en était qu'on n'avait pas compris que les anciennes façons de faire n'étaient plus nécessairement acceptables depuis l'entrée en vigueur de la *LPRPDÉ*.

Absence de mesures de sécurité convenables

Dans un cas l'an dernier, j'ai conclu qu'il n'était pas acceptable qu'une organisation ait recours au numéro de téléphone ou à l'année de naissance d'un titulaire de carte de crédit afin d'empêcher l'accès non autorisé aux renseignements personnels le concernant. Dans un autre cas, impliquant une perte de documents, j'ai conclu qu'une organisation n'avait pas pris des mesures convenables pour protéger les renseignements personnels durant le transfert des dossiers à un autre édifice. Et dans une autre affaire, j'ai découvert qu'une entreprise n'appliquait pas de mesures de contrôle opérationnelles indiquées dans le lieu de travail, afin d'assurer la confidentialité des fiches de paie des employés.

Dans ces cas et d'autres impliquant des manquements actuels ou potentiels à la protection des renseignements personnels, la question centrale concernait l'à-propos des mesures de sécurité prises par certaines organisations. Le principe 4.7 énonce que les renseignements personnels doivent être protégés par des mesures de sécurité qui conviennent au degré de sensibilité des renseignements. Suivant la nature des renseignements, les mesures de sécurité peuvent être de diverses formes, variant de mesures matérielles telles que des classeurs verrouillés ; à organisationnelles, comme les cotes de sécurité ; et aux mesures technologiques c.-à-d. l'utilisation de mots de passe et le chiffrement des données.

De toute évidence, les organisations doivent prendre plus au sérieux l'obligation de protéger les renseignements personnels, une fois qu'ils ont été recueillis.

Méconnaissance du fait que les employés ont également des droits à la vie privée

Il y a une preuve écrasante que certaines organisations qui sont des entreprises fédérales, lorsqu'elles apprennent que la *LPRPDÉ* vise la collecte, l'utilisation et la communication de renseignements personnels, concluent rapidement qu'il s'agit seulement des renseignements concernant leurs clients. Elles semblent ne s'être jamais

rendu compte qu'elles traitent également beaucoup de renseignements personnels concernant les individus qu'elles emploient, et ce, dans leurs activités administratives au jour le jour.

Par conséquent, certaines organisations ont réagi avec surprise lorsque des plaintes fondées en vertu de la *LPRPDÉ* ont été déposées contre elles – par des employés, actuels ou passés. D'un côté, les violations visées par ces plaintes découlaient du fait que l'organisation négligeait de tenir compte de ses employés au moment d'élaborer des politiques et procédures en matière de protection de la vie privée.

Réponses positives à mes recommandations

Malgré ce qui précède, j'estime qu'il est encourageant, une fois que les problèmes systémiques ont été signalés aux organisations, que la majorité d'entre elles acceptent habituellement volontiers les mesures correctives que je recommande et y donnent suite.

Dans l'ensemble, je suis satisfait des progrès réalisés jusqu'à date depuis l'entrée en vigueur de la *LPRPDÉ*, ainsi que des efforts déployés par les organisations pour assurer leur conformité.

Définitions aux termes de la *LPRPDÉ*

Non fondée : Cela signifie qu'il n'y a pas de preuve qui porte le Commissaire à la vie privée à conclure que l'organisation a violé la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*).

Fondée : Cela signifie que l'enquête a révélé que l'organisation n'a pas respecté une disposition de la *LPRPDÉ*.

Résolue : Cela signifie que l'organisation a pris des mesures correctives pour remédier à la situation, ou que le plaignant est satisfait des résultats de l'enquête menée par le Commissariat à la protection de la vie privée du Canada.

Abandonnée : Il s'agit d'une enquête qui a pris fin avant que toutes les allégations aient été pleinement examinées. Une affaire peut être abandonnée pour un nombre de raisons, par exemple, lorsque le plaignant n'est plus intéressé à poursuivre l'affaire.

Examens et pratiques en matière de vie privée

La *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*) m'autorise à vérifier la conformité des organisations privées si j'ai des « motifs raisonnables de croire » qu'elles contreviennent à une disposition de la *Loi* ou qu'elles ne respectent pas une recommandation énoncée dans l'annexe 1.

La Direction des examens et des pratiques en matière de vie privée du Commissariat effectuera des examens et des vérifications de conformité, aux termes de l'article 18 de la *LPRPDÉ*, en tenant compte des objectifs et des critères normalisés reconnus de vérification. Comme je l'ai mentionné dans mon précédent *Rapport annuel au Parlement*, je n'ai toujours pas entamé de vérification de cette sorte.

Devant les tribunaux

Aux termes de l'article 14 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (*LPRPDÉ*), un plaignant individuel a le droit, à l'issue de mon enquête, de déposer une demande d'audience à la Cour fédérale du Canada touchant toute question sur laquelle sa plainte était fondée ou qui est mentionnée dans le rapport du Commissaire. Ces questions doivent figurer dans les clauses à l'annexe et les articles de la *Loi* énumérés à l'article 14. Je peux également déposer une demande d'audience à la Cour pour toute plainte que j'ai entreprise. Depuis l'entrée en vigueur de la *Loi* le 1er janvier 2001, cinq demandes ont été déposées à la Cour fédérale.

Aux termes de l'article 15 de la *LPRPDÉ*, je suis autorisé à déposer une demande de comparution à la Cour fédérale. Je peux, avec le consentement du plaignant, demander directement à la Cour qu'elle ouvre une audience sur toute question visée à l'article 14 ; comparaître devant la Cour au nom de tout plaignant qui a présenté une demande en vertu de l'article 14 ; ou, avec l'autorisation de la Cour, comparaître comme partie à une instance engagée en vertu de l'article 14.

La liste qui suit n'est pas une liste exhaustive des demandes déposées auprès des cours, mais bien une liste des affaires comportant un intérêt particulier.

Mathew Englander c. Telus Communications Inc.

Il s'agit de la première demande qui a été déposée à la Cour fédérale aux termes de l'article 14 de la *LPRPDÉ*. M. Englander soutient que Telus utilise et communique les noms, adresses et numéros de téléphone de ses clients dans les pages blanches de son annuaire et ailleurs, à l'insu de ses clients et sans avoir obtenu leur consentement. En outre, Telus exige indûment des frais des clients qui demandent la « non-publication » de leur numéro de téléphone. M. Englander soutient que les mesures prises par Telus sont contraires aux paragraphes 5(1) et (3) de la *Loi*, ainsi qu'à plusieurs clauses de l'annexe 1 de la *Loi*.

État de la situation

Une date d'audience n'a pas encore été fixée.

Ronald G. Maheu c. IMS Health Canada et Commissaire à la protection de la vie privée du Canada

Ronald Maheu a demandé une audience à la Cour fédérale du Canada, soutenant qu'IMS Health Canada avait indûment communiqué des renseignements personnels en vendant des données sur les habitudes de prescription des médecins sans le consentement des intéressés.

État de la situation

Dans sa demande, M. Maheu avait demandé à la Cour de revoir ma « décision » dans cette affaire. J'ai déposé une requête m'opposant à la manière dont M. Maheu avait présenté sa demande, soutenant qu'aux termes de la *LPRPDÉ*, il revient à l'organisation concernée (IMS) dans l'affaire, et non au Commissaire à la protection de la vie privée, de justifier pourquoi elle ne devrait pas être obligée à modifier ses pratiques en vue de se conformer à la *Loi*. Le 12 février 2002, la Cour fédérale a ordonné à M. Maheu de déposer un avis de demande modifié en supprimant toute allégation et demande d'ordonnance à l'endroit du Commissariat, et lui a ordonné de formuler sa demande de façon qu'elle vise uniquement IMS Health Canada. J'ai également été autorisé, aux termes de l'alinéa 15*c)* de la *Loi*, à comparaître à titre de partie intimée afin d'appuyer ma conclusion dans cette affaire. Le 14 mai 2002, en réponse à une requête déposée par IMS, la Cour fédérale a ordonné à M. Maheu de verser une garantie financière. M. Maheu en a appelé avec succès de cette ordonnance.

Communications et sensibilisation du public

La *LPRPDÉ* a accru mes responsabilités ainsi que celles du Commissariat, et m'a donné ainsi qu'au Commissariat un rôle élargi et un mandat législatif plus important en vue de sensibiliser les Canadiens et Canadiennes et les organisations aux questions liées à la protection de la vie privée.

Afin de m'acquitter de ces nouvelles responsabilités et en guise de préparation aux activités de communication qui s'annoncent, les capacités de communication du Commissariat ont été étendues. Depuis, nous avons proactivement participé à diverses activités afin de sensibiliser davantage le public pour qu'il comprenne mieux les questions qui pourraient éventuellement menacer la vie privée des Canadiens et Canadiennes, pour les informer des protections légiférées relatives à la vie privée, et pour rappeler aux organisations du secteur privé quelles sont leurs responsabilités aux termes de la nouvelle législation.

Compte tenu de mes responsabilités mandatées aux termes de l'article 24 de la *Loi*, je me réjouis de la sensibilisation accrue au sujet des droits à la vie privée et des questions en matière de vie privée que ces activités semblent avoir suscitée.

Allocutions

Les conférences et les autres événements spéciaux, au Canada et à l'étranger, m'ont donné une occasion unique de rencontrer des Canadiens et Canadiennes et de sensibiliser davantage aux questions touchant la protection de la vie privée divers auditoires et milieux – des associations professionnelles et sectorielles, des groupes sans but lucratif et de défense d'intérêts, des universités et des événements publics.

Entre le 1er janvier 2001 et le 31 mars 2002, j'ai prononcé au total 55 allocutions alors que des cadres supérieurs du Commissariat en ont prononcé 35. Lors de ces événements, j'ai abordé certaines questions telles que la protection de la vie privée en milieu de travail, les enjeux de la génétique sur la vie privée, l'application de la *LPRPDÉ* et ses implications pour les entreprises, l'initiative Gouvernement en direct, mes profondes inquiétudes concernant la surveillance vidéo par les pouvoirs publics dans les endroits publics, ainsi que la nécessité d'équilibrer les droits à la vie privée et les objectifs en matière de sécurité dans la foulée des attaques terroristes aux États-Unis.

Lors de conférences internationales, j'ai eu l'occasion de partager ma perspective sur l'expérience canadienne avec des représentants et des défenseurs des droits à la vie privée d'autres pays.

Relations médiatiques

L'appétit des médias pour des nouvelles touchant la vie privée n'a cessé de croître. Notre analyse de la couverture médiatique révèle un intérêt croissant aux questions ainsi que la sensibilisation accrue au Commissariat. Le nombre d'appels de journalistes, qui se chiffre actuellement à environ 100 par mois, continue de s'accroître. Du 1er janvier 2001 au 31 mars 2002, j'ai accordé plus de 270 entrevues à des journalistes.

En plus de répondre aux demandes de renseignements et de commenter le droit à la vie privée et les droits des Canadiens et Canadiennes aux termes des lois fédérales connexes, le Commissariat a pris un nombre de mesures pour sensibiliser davantage à diverses questions par le biais des médias. Durant cette période, nous avons diffusé plus de 25 communiqués et avis aux médias, nous avons participé à bon nombre de rencontres avec des comités de rédaction de quotidiens de partout au pays, nous avons contribué des articles et d'autres renseignements à plusieurs publications, et nous avons appuyé les relations médiatiques lors de conférences, de rencontres publiques et d'autres événements spéciaux.

Documents de sensibilisation du public

En 2001, le Commissariat a produit deux guides en prévision de la demande des Canadiens et Canadiennes et d'entreprises pour de plus amples renseignements sur la *LPRPDÉ*. Notre *Guide à l'intention des citoyens* renseigne les Canadiens et Canadiennes sur leurs droits aux termes de la nouvelle *Loi*. Le *Guide à l'intention des entreprises* informe les organisations de leurs responsabilités prévues dans la *Loi*, de façon qu'elles puissent s'y conformer.

Le Commissariat reçoit tous les jours des demandes pour ces guides, et cette demande s'accroît. Non seulement ces documents sont-ils envoyés sur demande aux individus, ils sont aussi distribués lors de conférences et consultés sur notre site Web. Durant cette période, plus de 24 000 guides ont été distribués.

En plus du *Guide à l'intention des citoyens* et du *Guide à l'intention des entreprises*, le Commissariat a produit et distribué d'autres documents de sensibilisation et de promotion, notamment des signets, des affiches, des fiches d'information, des rapports annuels, et des exemplaires des deux lois fédérales sur la protection des renseignements personnels.

Nous envisageons actuellement d'autres lieux convenables où offrir aux Canadiens et Canadiennes les guides et d'autres documents.

Publicité

La publicité est un autre outil important que le Commissariat utilise pour sensibiliser le public et lui permettre de mieux comprendre les questions touchant la protection de la vie privée.

En 2001, nous avons fait paraître des publicités dans les quotidiens et les journaux communautaires. Les annonces renfermaient des renseignements sur la nouvelle *Loi* et son application aux entreprises sous réglementation fédérale.

En 2002, nous avons lancé une autre campagne de publicité nationale. Des messages radiophoniques ont été produits en français et en anglais, et ont été diffusés sur les principales chaînes sur tous les marchés au pays. Ces annonces radiophoniques mettaient l'accent sur les droits des Canadiens et Canadiennes que leur confère la nouvelle *Loi* ainsi que sur le rôle du Commissariat dans la protection de ces droits.

Les deux campagnes publicitaires ont permis de joindre des millions de Canadiens et Canadiennes, et ont presque fait doubler le nombre de demandes de renseignements acheminées au Commissariat.

Demandes de renseignements du public

La Division des communications et des politiques répond à des milliers de demandes provenant du grand public, qui s'adresse au Commissariat afin d'obtenir des conseils et de l'aide pour toutes sortes de questions liées à la protection des renseignements personnels.

Site Web

Dans un esprit d'ouverture et de transparence, tous les efforts sont déployés afin d'assurer que les renseignements nouveaux et utiles sont affichés sur le site Web du Commissariat sur une base régulière et en temps opportun. De nouveaux éléments tels que des discours, des communiqués, des feuilles d'information, des rapports choisis et des sommaires de cas alimentent le site pour qu'il soit à jour et intéressant.

L'an dernier, étant donné que les organisations cherchaient à mieux comprendre les modalités de l'application de la *LPRPDE*, une nouvelle section, intitulée « Conclusions du Commissaire », a été ajoutée à notre site. Les sommaires de mes conclusions y sont affichés afin d'orienter les entreprises et le milieu juridique.

En 2001, le site Web a été remanié entièrement et le nombre de visites sur le site Web s'est progressivement accru et a presque doublé après octobre 2001. Au cours de cette période, le site a reçu en moyenne 16 000 visites par mois.

Activités de communication

1er janvier 2001 - 31 mars 2002

Activité		Nombre
Allocutions du Commissaire à la protection de la vie privée		55
Allocutions des cadres supérieurs		35
Communiqués		25
Entrevues avec les médias		270
Documents distribués		**34 036**
Guide à l'intention des entreprises	14 170	
Guide à l'intention des citoyens	10 666	
Autres (rapports annuels, signets, fiches d'information, exemplaires de lois, etc.)	9 200	
Nombre moyen de visites du site Web par mois		16 079

Demandes de renseignements par catégorie en vertu de la *Loi sur les renseignements personnels*

1er avril 2001 - 31 mars 2002

Objet	Nombre
Adoption, généalogie	35
Accès aux renseignements personnels *	504
Recensement	297
Collecte, utilisation et communication *	224
Questions liées au consentement *	25
Corrections *	18
Dossiers criminels, pardons	203
Formulaire de déclaration du voyageur (E-311) **	26
Armes à feu	76
Application de la loi *	60
Dossiers médicaux **	98
Absence de compétence (niveau fédéral)	983
Commissariat à la protection de la vie privée du Canada *	111
Renseignements personnels sur la santé *	49
Loi sur la protection des renseignements personnels, interprétation et processus	6 988
Demande de publications	189
Renvois à l'extérieur du CPVP	3 240
Numéro d'assurance sociale	410
Surveillance vidéo *	50
Surveillance dans les milieux de travail *	13
Appels de députés du Parlement	31
Autres	642
Total	14 272

* Ces catégories ont été compilées de janvier à mars 2002 seulement.
** Ces catégories ont été compilées d'avril à décembre 2001 seulement.

Demandes de renseignements par catégorie en vertu de la *LPRPDÉ*

1er janvier 2001 - 31 décembre 2001

Objet	Nombre
Dossiers criminels	31
Tests de dépistage de drogues	3
Chiffrement de données	7
Institutions fédérales	1 609
Vol d'identité	38
Demandes de renseignements	2 744
Interception – surveillance	154
LPRPDÉ, interprétation et processus	2 151
Secteur de compétence	2 103
Marketing	462
Dossiers médicaux	144
Demandes de publication	679
Numéro d'assurance sociale	1 902
Télécommunications	827
Transports	152
Appels de députés du Parlement	7
Autres	388
Total	**13 401**

Troisième partie
Services de gestion

Afin d'administrer la mise en œuvre de la *LPRPDÉ* et en raison du mandat élargi aux termes de la *Loi*, le Commissariat a obtenu des ressources accrues, à la fois humaines et financières.

Le 1er avril 2001, le budget du Commissariat a augmenté, passant de 8,7 millions à 11,1 millions de dollars par rapport à l'exercice antérieur, et celui-ci sera maintenu en vue d'appuyer les activités suivantes au cours du prochain exercice :

- L'augmentation des activités de communications, d'enquêtes et de plaintes ;
- L'augmentation du nombre d'enquêteurs, de vérificateurs et d'agents d'évaluation des facteurs relatifs à la vie privée afin d'aborder des questions touchant les deux lois fédérales sur la protection des renseignements personnels ;
- Le prolongement de nos heures de travail, de 9 h à 17 h dans tous les fuseaux horaires du Canada ;
- L'établissement d'un cadre de gestion solide qui comprend les fonctions d'enquête et de vérification du Commissariat ; et
- L'établissement le 1er avril 2002 de la Direction des services de gestion au sein du Commissariat, qui est chargée des questions touchant la technologie de l'information, les ressources humaines, les finances et l'administration (anciennement, les services de gestion étaient partagés avec le Commissariat à l'information).

Une fois que la *LPRPDÉ* sera pleinement en vigueur le 1er janvier 2004, un cadre financier aux fins de financement sera présenté au Secrétariat du Conseil du Trésor afin de justifier des dépenses futures.

Ressources

1er avril 2001 - 31 mars 2002

	ETP	Dépenses globales	Pourcentage du total
Protection de la vie privée	93	9 435 901 $	82 %
Services de gestion	15	2 021 867 $	18 %
Total	**108**	**11 457 768 $**	**100 %**

Nota : ETP signifie « équivalent temps plein » ou le personnel à temps plein en date de mars 2002.

Dépenses détaillées

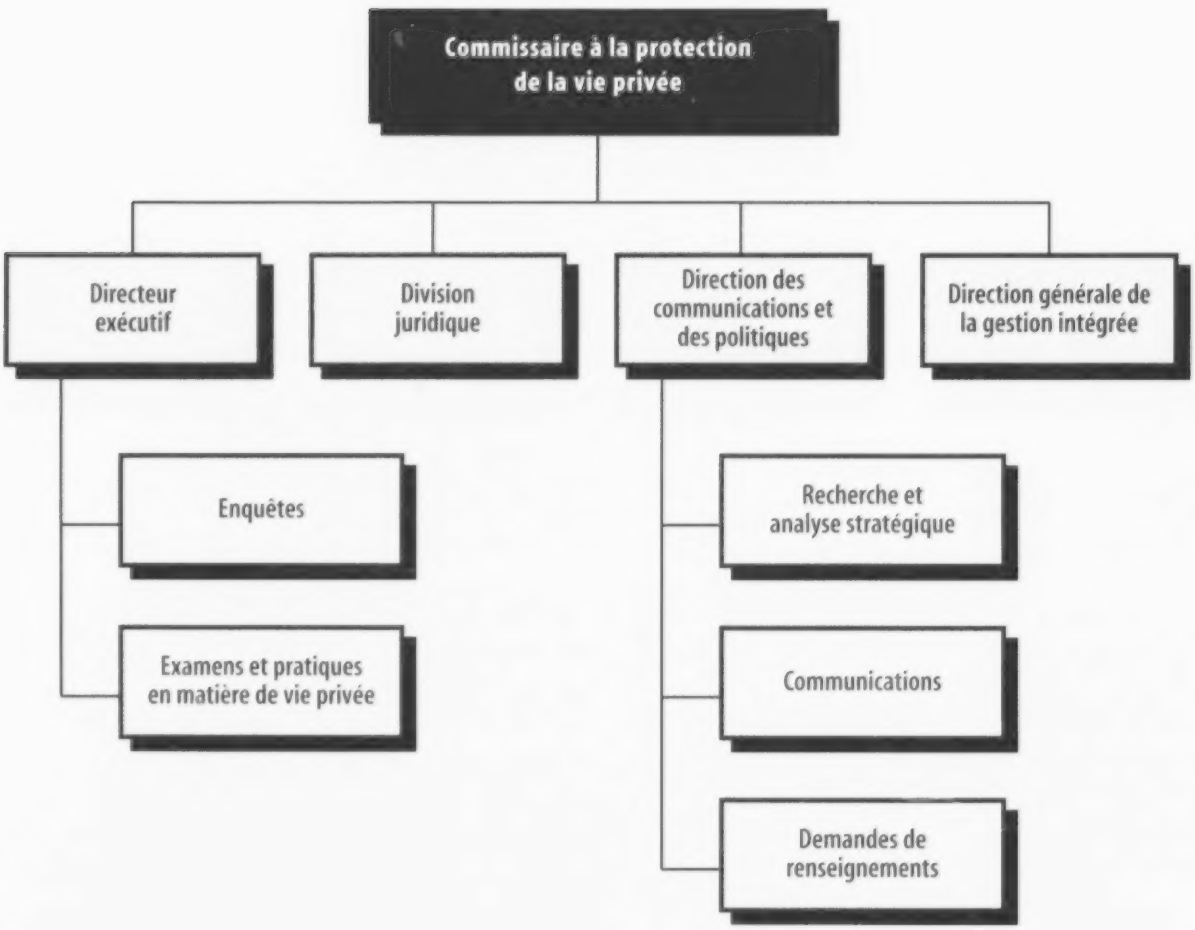
1er avril 2001 - 31 mars 2002

	Protection de la vie privée	Services de gestion	Total
Salaires et traitements	5 101 779 $	1 078 633 $	6 180 412 $
Cotisations au régime d'avantages sociaux des employés	1 172 850	167 150	1 340 000
Transports et communications	446 109	132 985	579 094
Information	1 566 375	7 502	1 573 877
Services professionnels	656 962	223 749	880 711
Locations	11 412	20 923	32 335
Réparations et entretien	50 453	19 920	70 373
Approvisionnements et fournitures	99 053	40 494	139 547
Achat de machines et d'équipements	298 673	330 147	628 820
Autres subventions et paiements	32 235	364	32 599
Total	**9 435 901 $**	**2 021 867 $**	**11 457 768 $**

Nota :

1. Les dépenses totales correspondent aux comptes publics.
2. Les dépenses des Services de gestion étaient réparties équitablement entre le Commissariat à la protection de la vie privée du Canada et le Commissariat à l'information du Canada, qui partagent ces dépenses.
3. À compter du 1er avril 2002, les Services de gestion font partie du Commissariat leurs services ne sont plus partagés avec le Commissariat à l'information du Canada.

Structure organisationnelle



- À compter du 1er avril 2002, les Services de gestion font partie du Commissariat leurs services ne sont plus partagés avec le Commissariat à l'information du Canada.